ØKT MOTSTANDSKRAFT OG KONKURRANSEDYKTIGE VIRKSOMHETER

HVA BESLUTNINGSTAKERE MÅ GJØRE FOR Å STYRKE EGEN VIRKSOMHET, MED DYPDYKK I KRAFTSEKTOREN OG MAT- OG PROSESSERINGSINDUSTRIEN I NORGE

Radar.

cisco

INNHOLD

Analytiker og redaktør

Head of Business Development, Radar Norway, Iselin Paulsen
E-post: iselin.paulsen@radargrp.com

INTRODUKSJON

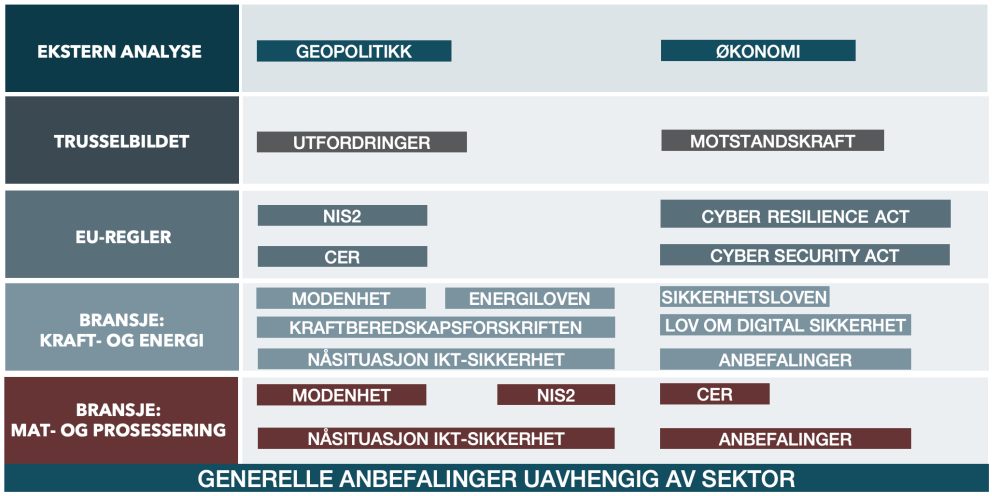
Radar skriver denne rapporten på oppdrag fra Cisco for å belyse hvilke utfordringer og muligheter som ligger foran norske beslutningstakere innen IT og teknologi, med dypdykk i utfordringene og mulighetene for kraft- og energibransjen og mat- og prosesseringsindustrien i Norge.

Eksterne faktorer som geopolitikk, regulatorisk utvikling og økonomisk situasjon påvirker norske virksomheter i stadig større grad. Samtidig ligger det både begrensninger og muligheter i modenhet i norske virksomheter, og det øker betydningen av IT som muliggjører for innovasjon, forretningsutvikling og motstandskraft.

Rapporten retter seg mot beslutningstakere for veiledning og innsikt om økt konkurransekraft gjennom sterkere virksomheter som er mer motstandsdyktige. Rapporten redegjør for det nye trusselbildet, og diskuterer hvordan nye lover og regler påvirker grunnlaget for videreutvikling av virksomhetene. Vi vil beskrive utfordringer og muligheter og komme med konkrete forslag til beslutninger for å styrke virksomhetenes konkurransekraft og motstandsevne.

Hvordan lese rapporten?

Rapporten starter med en geopolitisk og økonomisk analyse, før vi går inn på trusselbildet og relevante EU-regler. Deretter presenterer vi bransjeanalyse på henholdsvis kraft- og energisektoren og mat- og prosesseringsindustrien, med tilhørende gjennomgang av modenhet, nasjonale regler og IKT-sikkerhet for begge sektorer. Vi presenterer også tilhørende anbefalinger per bransje, før vi avslutter med generelle anbefalinger på tvers av sektorer. Rapportens oppbygging er illustrert her:



OPPSUMMERING

Den utfordrende geopolitiske og økonomiske situasjonen har i mange land ført til **raskere beslutningsprosesser**, og viktige **regelendringer og direktiver** om økt motstandskraft kommer på løpende bånd. Bedriftenes kostnader har økt mye de siste årene, og høy lønnsvekst og en svakere krone bidrar til å holde prisveksten oppe. Dette påvirker norske beslutningstakere sterkt, og norske virksomheter må sørge for å ha sikre, trygge og gode systemer som gjør at virksomheten kan møte **økt trusselnivå, økte kostnader og økte regulatoriske og administrative krav.**

Vi står i dag overfor en **systematisk sikkerhetstrussel** drevet av aktører med politiske, militære eller økonomiske interesser. Norske virksomheter er viktige i det **forebyggende sikkerhetsarbeidet**. Verdier med betydning for nasjonal sikkerhet eies og forvaltes i hovedsak av virksomhetene, både private og offentlige.

Rapporten viser et behov for å styrke norske virksomheters motstandskraft, som er definert slik:

Motstandskraft er en organisasjons evne til å tilpasse seg endrede forhold, motstå forstyrrelser og komme seg raskt etter uheldige hendelser. I sammenheng med cybersikkerhet handler cybermotstandskraft spesielt om en organisasjons evne til å minimere virkningen av cyberhendelser og gjenopprette operative systemer for å opprettholde forretningskontinuitet.»

Et stort antall norske og europeiske regler kommer på løpende bånd fremover for å styrke samfunnets og virksomhetenes motstandskraft. En fellesnevner for reglene som kommer, er **økte krav til kompetanse om risiko og økt ledelsesansvar for økt motstandskraft i virksomheter.**

De viktigste *europeiske* reglene for norske beslutningstakere på sikkerhetsområdet er: **NIS2-direktivet, CER-direktivet**, **Cybermotstandsdirektivet** og **Cybersikkerhetsloven.**

I denne rapporten dypdykker vi inn i to sektorer som er viktige for Norge: Kraft- og energisektoren og mat- og prosesseringsindustrien. Begge sektorer har høy utbredelse av IT/OT- systemer, og har komplekse verdikjeder som utgjør sårbarheter som kan utnyttes. Kraft- og energisektoren har imidlertid kommet lengre enn mange andre sektorer hva gjelder digital modenhet, og er også spesifikt nevnt som essensiell og viktig sektor i de nye europeiske reguleringene NIS2- og CER-direktivet.

Tilsynsregimet og regelverksutviklingen er derimot ulik for de to sektorene. Mat- og prosesseringsindustrien har i motsetning til kraftsektoren ikke tidligere hatt et strengt regelverk på IKT-sikkerhet, men blir fremover omfattet av nye regler som CER-direktivet og NIS2-direktivet.

Vi belyser nærmere hvilke utfordringer og muligheter som gjelder for disse to sektorene. Til slutt i rapporten oppsummerer vi bransjegjennomgangen, og kommer med anbefalinger både til de utvalgte bransjene, men også generelle anbefalinger som gjelder på tvers av sektorer.

Kraft- og energisektoren

Kraftforsyningen eier og driver en av Norges mest **samfunnskritiske infrastrukturer**. Både myndighetene og ledelse i virksomheter har derfor høyt fokus på informasjonssikkerhet, et forhold som nett- og produksjonsselskapene må forholde seg til på en forsvarlig og hensiktsmessig måte.

Sentrale nasjonale regler som gjelder for kraft- og energibransjen er: **Energiloven**, **sikkerhetsloven** og **kraftberedskapsforskriften**, samt **ny lov om digital sikkerhet**. Reglene omfatter krav til planlegging, risikovurdering, beredskapsforberedelser, øvelser og rapportering for å styrke sektorens evne til å håndtere ulike typer hendelser, fra tekniske feil til eksterne påvirkninger.

Et sterkt og strengt regelverk er alene er ikke nok til å styrke motstandskraften hos virksomhetene i kraftsektoren. Faktisk etterlevelse av funksjonskravene i regelverket krever et **ordentlig, systematisk og risikobasert sikkerhetsarbeid**.

Rapportens gjennomgang av nåsituasjonen for IKT-sikkerhet viser at kraftsektoren har flere utfordringer knyttet til IKT-sikkerhet og motstandskraft mot hendelser, samt evne til å håndtere hendelser. Mange virksomheter opplever utfordringer med risikostyring, tjenesteutsetting og overvåking og logging. Det er også flere som uttrykker utfordringer med identifisering av kraftsensitiv informasjon, gjennomføring av sikkerhetsrevisjoner og evaluering og testing. Vår analyse viser at det er behov for **økt motstandskraft og økt modenhet i risikostyring i kraftsektoren.**

Våre anbefalinger til beslutningstakere i kraft- og energisektoren er:

1. Integrer sikkerhet i virksomhetens aktiviteter og etablér styringssystem for informasjonssikkerhet
2. Les sikkerhetsloven, energiloven samt kraftberedskapsforskriften. Bruk veilederne.
3. Les veileder for risikovurderinger og informasjonssikkerhet i IT- og OT-systemer
4. Bruk sjekklisten for IKT-sikkerhet i anskaffelser og tjenesteutsetting
5. Bruk NSMs grunnprinsipper for IKT-sikkerhet
6. Hold deg informert om kommende lover

Mat- og prosesseringsindustrien

Norge har et høyteknologisk og transportintensivt matproduksjons- og distribusjonssystem. Økt digitalisering og avhengighet av teknologi i alle faser av produksjon, distribusjon og salg av mat, gjør at cyberangrep kan forstyrre og skade hele matforsyningsprosessen.

Rapporten viser at matsektoren må forholde seg til økte krav til ledelsesinvolvering, økte investeringer i sikkerhet, og økte krav til leverandørstyring og hendelsesrapportering. Kommende EU-regler som NIS2-direktivet og CER-direktivet vil gjøre det enda viktigere for mat- og prosesseringsundustrien å ha et **ordentlig, systematisk og risikobasert sikkerhetsarbeid**.

Våre anbefalinger til beslutningstakere i mat- og prosesseringsindustrien er:

1. Innpass sikkerhet i virksomhetens aktiviteter og etablér styringssystem for informasjonssikkerhet
2. Bruk NSMs grunnprinsipper for IKT-sikkerhet
3. Les NSMs rapport og tiltak mot de ti vanligste sårbarhetene i norske IT-virksomheter
4. Les NVEs veileder for risikovurderinger og informasjonssikkerhet i IT- og OT-systemer
5. Sørg for god IKT-sikkerhet i anskaffelser og tjenesteutsetting
6. Gjennomgå minimumskravene i CER-direktivet og minimumstiltakene for cybersikkerhet ihht NIS2
7. Hold deg informert om kommende lover

Generelle anbefalinger alle beslutningstakere uavhengig av sektor
Tette koblinger og avhengigheter, og rask innføring av ny teknologi, sammen med komplekse og lange verdikjeder i flere sektorer, gir økt omfang av reguleringer, økte angrepsflater og til sist et mer krevende sikkerhetsarbeid. Her er våre generelle anbefalinger til norske beslutningstakere uavhengig av sektor.

Virksomheters motstandskraft må økes!
Virksomhetene må evne å tilpasse seg nye og endrede forutsetninger, og kunne håndtere eventuelle forstyrrelser og må samtidig ha evne til å komme seg raskt etter uønskede hendelser.

Økt profesjonalisering av risikostyring i virksomheter
Flere ansatte og ledere vil tilegne seg økt kompetanse på risikostyring, og med økt profesjonalisering kommer også økte krav til leveranser i ledergrupper.

Risikostyring er et ledelsesansvar!
NIS2-reglene tydeliggjør ledelsens ansvar, se spesielt artikkel 20 og 21. Dette kan gjøre det enklere å prioritere sikkerhetsfaglige råd i virksomhetene, og kan bidra til at det blir enklere å sikre investeringer til nødvendige sikkerhetstiltak.

Økt kamp om sikkerhetsressurser og kompetanse
Økte minimumskrav forventes å gi økt kamp om ressursene innen sikkerhetskompetanse, økt etterspørsel etter sikkerhetstjenester, og økt etterspørsel etter nearshoring og offshoring som følge av at NIS2-regelverket gjelder for hele EU.

Økte kostnader og behov for flere investeringer
NIS2-direktivet alene gir økte kostnader for virksomhetene. EUs egne tall antyder en **kostnadsøkning på 22 %** for de virksomheter som ikke tidligere har vært omfattet av NIS1, og en **kostnadsvekst på 12 %** for de virksomheter som fra før av er omfattet av NIS1. Direktivet innebærer også økte investeringer i opplæring og kompetanse. I tillegg kommer økte reguleringer og tilhørende investeringer som følge av eksempelvis CER-direktivet.

Økt behov for kjøp av «secure by design» tjenester
Det blir økt behov for kjøp av ferdig pakketerte «Secure by design»- tjenester. Dette er produkter der sikkerheten til kundene er et kjernekrav, ikke bare en teknisk funksjon.

DET GEOPOLITISKE BILDET

Det er nå en kompleks geopolitisk situasjon med krig i Europa, der USA er en kraftig bidragsyter samtidig som kløften mellom USA og Kina blir større i Sør-Kina-havet. Det pågår også en konflikt mellom Israel og Palestina. Teknologi og digitalisering har nå også en sikkerhetspolitisk dimensjon, slik også Forsvarskommisjonen påpeker i sin proposisjon NOU 2023: 14.10

I 2024 er det et såkalt "supervalgår", der hele 40 % av verdens befolkning kan bruke sin stemmerett ved valg. Det gjør at det geopolitiske bildet får enda større innvirkning på utviklingen hos stormaktene. Det forestående presidentvalget i USA kan medføre økte spenninger internt i USA, og det kan føre til ytterligere forsinkelser og utsettelser av sårt tiltrengt støtte til Ukraina.

Slaget mellom stormaktene står ikke bare på slagmarken, men også på områdene teknologi, energi og kompetanse. Det pågår også store investeringer i handel i USA og EU, der USA med Inflation Reduction Act investerer store penger for en økt hastighet på grønn omstilling. Investeringene utgjør den største klima- og energisatsingen i amerikansk historie, med hele 369 milliarder dollar som går til fornybar energi og nullutslippsteknologi.

Krigen i Ukraina kan eskalere videre og påføre verdens råvare- og energimarkeder ytterligere påkjenning. Stormaktrivaliseringen mellom USA og Kina kan tilta ytterligere, og latente spenninger i Øst-Asia kan eskalere. Konflikten mellom Israel og Palestina kan få ringvirkninger i Midt-Østen. En eskalering av konfliktene vil få store konsekvenser for internasjonal aktivitet og handel.

Den industrielle konkurransen mellom Kina og USA begrenser seg ikke til forsvarsindustrien, men påvirker hele verdikjeder fra råmaterialer til programvare. I de kommende årene vil verdikjedene bli søkt sikret av stater og eiere for å unngå avhengigheter og sårbarheter.

Teknologiske skifter skaper fundamentale endringer, spesielt innen økonomi, demografi og arbeidsmarked, men også militært. Ifølge Forsvarskommisjonen må Norge ha en mer strategisk tilnærming til utvikling og beskyttelse av kompetanse og teknologi.

De sterke geopolitiske, regulatoriske og teknologiske endringene, gjør at Norge må samarbeide ytterligere med andre aktører både internasjonalt, i Europa og i Norden. Ifølge analysebyrået Radar har den geopolitiske situasjonen ført til raskere beslutningsprosesser enn vi tidligere har vært vant til, og Norge må intensivere sitt samarbeide med andre for ikke å bli akterutseilt. Viktige regelendringer og direktiver har kommet og kommer på løpende bånd på områder som er viktig for Norge, noe vi har sammenfattet i Bilag A i denne rapporten.

DEN ØKONOMISKE SITUASJONEN

Norges Bank vurderer at renten er høy nok til å få prisveksten ned til målet på 2 prosent innen rimelig tid. Pengepolitikken virker innstrammende, og det er lav vekst i norsk økonomi. Prisveksten avtar, men den er fortsatt klart over målet. Bedriftenes kostnader har økt mye de siste årene, og høy lønnsvekst og en svakere krone bidrar til å holde prisveksten oppe. [1]

Næringslivets hovedorganisasjons medlemsundersøkelse fra mai 2024, viste at 23 prosent av respondentene mener at markedssituasjonen var god, mens 22 prosent oppga situasjonen som dårlig. I april var det motsatt, da oppga 22 prosent at situasjonen var god, mens 23 prosent oppga situasjonen som dårlig. Nettobalansen for utsiktene har derfor bedret seg noe fra april til mai fra -7 prosent til -5 prosent. [2]

NHOs ferskeste økonomiske overblikk beskriver hvordan kostnadssjokket etter pandemien og krigen i Ukraina ble forsterket av høy kapasitetsutnytting, flaskehalser i verdikjedene og lav ledighet. Tallene tyder nå på at det opprinnelige kostnadssjokket er unnagjort og prisstigningen kan ha toppet ut i

[1] Norges Bank, rentebeslutning mai 2024: https://www.norges-bank.no/tema/pengepolitikk/Rentemoter/2024/mai-2024/#:~:text=Norges%20Banks%20komit%C3%A9%20for%20pengepolitikk%20og%20finansiell%20stabilitet,god%20stund%20fremover%2C%20sier%20sentralbanksjef%20Ida%20Wolden%20Bache.

[2] NHO, medlemsundersøkelse mai 2024: https://www.nho.no/tema/okonomisk-politikk-og-analyse/artikler/2024/nhos-medlemsundersokelse-bade-situasjon-og-utsikter-noe-forbedret-i-mai/

mange land. NHO peker på at det kan ta tid å bringe prisveksten ned mot målet, da kapasitetsutnyttingen fortsatt er høy.

Dette har en sterk påvirkning på norske virksomheter og norske beslutningstakere, som i en situasjon med kostnadspress, samtidig må sørge for å ha sikre, trygge og gode systemer som gjør at virksomheten kan møte økt trusselnivå, økte regulatoriske og administrative krav. Norske virksomheter må ha god risikostyring, og må investere i økt og riktig kompetanse, økt modenhet og moderne og muliggjørende teknologi.

OPPSUMMERING GEOPOLITIKK OG ØKONOMI

Gjennomgangen av geopolitisk og økonomisk utvikling viser at teknologi og digitalisering nå har en sikkerhetspolitisk dimensjon, og at slaget mellom stormaktene ikke lengre kun står på slagmarken, men på områdene **økonomi, teknologi og energi**. Dette øker verdien av sikre verdikjeder. Den utfordrende geopolitiske situasjonen har ført til **raskere beslutningsprosesser**, og viktige **regelendringer og direktiver** om økt motstandskraft kommer på løpende bånd. Bedriftenes kostnader har økt mye de siste årene, og høy lønnsvekst og en svakere krone bidrar til å holde prisveksten oppe. Dette påvirker norske beslutningstakere sterkt, og norske virksomheter må sørge for å ha sikre, trygge og gode systemer som gjør at virksomheten kan møte **økt trusselnivå, økte kostnader og økte regulatoriske og administrative krav.**

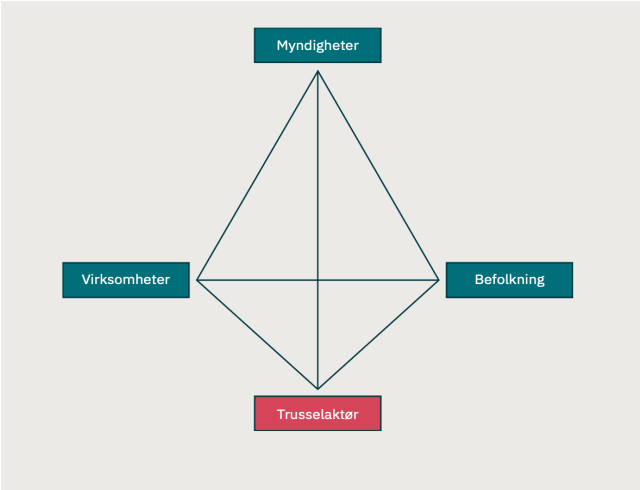
For å belyse eksisterende og kommende trusselbilde ytterligere, beskriver vi i neste del av rapporten hvilke aktører og utfordringer virksomhetene møter innenfor sikkerhet, samt europeiske regulatoriske krav på området, før vi skal dypdykke i situasjonen for kraft-og energibransjen og mat- og prosesseringsindustrien.

DET NYE TRUSSELBILDET- SYSTEMATISKE CYBERSIKKERHETSTRUSLER

Cyberangrep er blant de raskest voksende formene for kriminalitet, og det blir stadig mer komplekst og kostbart å beskytte seg mot dem. Vi står i dag overfor en **systematisk sikkerhetstrussel** drevet av aktører med politiske, militære eller økonomiske interesser. Cyberkriminelle har økt evne og interesse for å angripe digitale leverandørkjeder, noe som får store konsekvenser gjennom hele IT-økosystemet.
Risikoen mot virksomhetene øker når kostnadene og konsekvensene av å bli rammet blir stadig høyere. EU's sikkerhetsorgan, ENISA, anslår at mediankostnaden for en IT-hendelse i EU var i overkant av 2 millioner NOK i løpet av 2022. Dette er en fordobling av kostnadene på ett år.

AKTØRER SOM KAN PÅVIRKE SIKKERHETSTILSTANDEN

Myndighetene, virksomhetene og befolkningen er tre aktører i samfunnet som har ansvar for, eller kan påvirke, sikkerhetstilstanden. Med komplekse utfordringer og et utfordrende trusselbilde er det viktig å være bevisst på samspill og avhengigheter mellom aktørene. Nasjonal sikkerhetsmyndighet har en god illustrasjon på dette samspillet:



Sikkerhetsdiamanten. Kilde: NSM, Nasjonal sikkerhet mot 2030.

I denne rapporten gir vi råd til **virksomhetenes** rolle. Norske virksomheter er viktige i det **forebyggende sikkerhetsarbeidet**. Verdier med betydning for nasjonal sikkerhet eies og forvaltes i hovedsak av virksomhetene, både private og offentlige. Med støtte fra norske myndigheter, skal **virksomhetene kunne avdekke, forhindre og håndtere sikkerhetstruende hendelser**. Virksomheter må også ha evne til å **gjenopprette en sikker tilstand** for verdiene de forvalter.

For å gi et godt bilde på hvilket trusselbilde virksomhetene møter, går vi først gjennom trusselaktører norske virksomheter må beskytte seg mot.

TRUSSELAKTØRER

Cybertruslene som rettes mot norske aktører og interesser er mangfoldige og kommer fra ulike typer trusselaktører med ulike drivkrefter.

Statlige aktører eller statsstøttede aktører utgjør en betydelig trussel. I tillegg til å påføre direkte skade, kan de engasjere seg i aktiviteter som etterretning og påvirkningskampanjer med mål om å undergrave tilliten til samfunnets institusjoner eller påvirke det norske samfunnet i tråd med egne nasjonale interesser.

Kriminelle aktører er primært drevet av økonomiske interesser og er raske til å omfavne ny teknologi for å finne nye måter å tjene penger på. Mens målene til disse aktørene ikke er primære som for statlige aktører, styres deres handlinger av maksimal avkastning med minimal risiko. Organisatorisk begynner de å ligne mer på oppstartsbedrifter enn kriminelle gjenger på grunn av tjenestefiseringen av cyberkriminalitet, en økende grad av spesialisering og en voksende infrastruktur for å drive kriminell virksomhet.

Hacktivister er enkeltpersoner eller grupper drevet av ideologiske motiver eller politiske interesser. Hacktivister driver ofte med «enklere» aktiviteter som DDoS (overbelastningsangrep), som ikke forårsaker permanent skade, men som har som mål å skape oppmerksomhet. Slike angrep påvirker tilgjengeligheten av tjenester og bidrar også til å skade tilliten til de berørte virksomhetene.

VIRKSOMHETENES CYBERSIKKERHETSUTFORDRINGER

Den digitale akselerasjonen skaper utfordringer og trusler som virksomheter må håndtere og beskytte seg mot gjennom **systematisk sikkerhetsarbeid**. Her er noen av de vanligste cyberhendelsene som rammer virksomheter og samfunnet:

Eksempler på eksterne trusler mot virksomheter grunnet økt digitalisering[3]		
Løsepengevirus	Digitale tilganger eller data blir stjålet og løsepenger kreves av de kriminelle.	Vanlig hendelse Økende trend
Skadelige programmer	Skadelig kode som gir uatorisert tilgang som har en negativ innvirkning på et systems konfidensialitet, integritet eller tiljgengelighet.	Vanlig hendelse Økende trend
Social Engineering	Utnytting av menneskelige feil eller menneskelig adferd for å sikre seg uautorisert tilgang til informasjon eller tjenester. (Inkluderer phishing, honeytraps etc)	Vanlig hendelse Økende trend
Trusler mot data	Datainnbrudd, som er en villet ondsinnet handling fra en cyberkriminell med mål om uautorisert tilgang til og publisering av sensitive, konfidensielle eller beskyttede data. Datalekkasje er en hendelse som gjennom for eksempel feilkonfigurering, sårbarheter eller menneskelige feil kan utløse tap av, eller synliggjøring av, data som er sensitive, konfidelsielle eller beskyttede data.	Vanlig hendelse Økende trend
Trusler mot tilgjengelighet, Denial of Service og trusler mot internettilgang	Overbelastningsangrepe (DDoS) som gjør at brukerne ikke får tilgang til relevante data, tjenester eller andre ressurser. . Metoden har blitt industrialisert og har også blitt benyttet som verktøy i den pågående angrepskrigen fra Russland i Ukraina Trusler mot internettilgang er tilsiktede eller ikke-tilsiktede disrupsjoner av internett eller elektronisk kommunikasjon som resulterer i avbrudd i tilgang til internett, sensur eller nedstengning av internett. Slike disrupsjoner kan være myndighetsstyrte nedstengninger, naturhendelser, cyberangrep eller militærhendelser. Slike truser blir stadig mer varierte og øker.	Vanlig hendelse Økende trend
Manipulering og desinformasjon	Bruk av for det meste ulovlig adferd som truer eller har potensial til å true verdier, prosedyrer og politiske prosesser. Denne aktivitet er manipulativ, og utført på en tilsiktet og koordinert måte. Brukes av både statlige og ikke-statlige aktører.	Økende trend
Leverandørkjedeangrep	Et angrep som både skader leverandør og kunde, og får raskt stort skadepotensial grunnet den store kundebasen for slike angrep.	Økende trend

Det digitaliserte samfunnet består av en tett sammenkoblet infrastruktur som Norge er avhengig av. Det er viktig at samfunnskritiske virksomheter sammen hever sin forsvarsevne, ikke bare for å beskytte sin egen virksomhet, men for å bidra til å styrke hele verdikjeden og dermed samfunnets motstandskraft som helhet. En kjede er ikke sterkere enn svakeste ledd, og EU-kommisjonen har derfor sett seg nødt til å lovregulere ytterligere arbeidet med cybersikkerhet i Europa. Målet er å øke samfunnets og **virksomhetenes motstandskraft**.

VIRKSOMHETERS MOTSTANDSKRAFT (RESILIENCE)

Gjennomgangen ovenfor, viser at det er et behov for å **styrke norske virksomheters motstandskraft i alle sektorer**.

[3] ENISA, Threat landscape 2023: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Definisjonen[4] vi benytter på motstandskraft er:

> "Motstandskraft er en organisasjons evne til å tilpasse seg endrede forhold, motstå forstyrrelser og komme seg raskt etter uheldige hendelser. I sammenheng med cybersikkerhet handler cybermotstandskraft spesielt om en organisasjons evne til å minimere virkningen av cyberhendelser og gjenopprette operative systemer for å opprettholde forretningskontinuitet.»

Kilde: Cisco, What is Cyber Resilience

I denne rapporten benytter vi Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet som eksempel på hvilke aktiviteter man må ha kontroll på for å sikre økt motstandskraft i en virksomhet.

De fire trinnene i NSMs grunnprinsipper for IKT-sikkerhet gir råd for å beskytte informasjonssystemer, data og tjenester mot uautorisert tilgang, skade eller misbruk. Kilde: NSM.[5]

Det er altså ikke nok med reaktiv håndtering av hendelser, virksomhetene må også ha rutiner for forebyggende kartlegging, beskyttelse og oppdaging, samt rutiner for håndtering av hendelser og trusler.

EU og Norge bruker regulatoriske kraft for å oppnå både **økt motstandskraft**, **økt konkurransekraft, økonomisk vekst og effektivt samarbeid** mellom medlemslandene. Innføringen av ny cybersikkerhetslov, nye krav til produkters sikkerhet, og den nye loven om digital sikkerhet (i tråd med NIS 1 direktivet) samt det nye NIS2-direktivet vi gjennomgår nedenfor, er politiske svar på den økte trusselen.

I det følgende gjennomgår vi derfor utvalgte relevante EU-regler som påvirker beslutningstakere i Norge. Vi viser også de viktigste norske sektorvise regler i vår bransjegjennomgang av kraft- og energi og mat- og prosesseringsindustri.

REGLER SOM PÅVIRKER NORSKE IT-BESLUTNINGSTAKERE

Et stort antall norske og europeiske regler kommer på løpende bånd fremover. En fellesnevner for reglene som kommer, er **økte krav til kompetanse om risiko og økt ledelsesansvar for økt motstandskraft i virksomheter.** I et følgende gjennomgår vi de viktigste **europeiske** regler på IT-sikkerhets- og etterlevelsesområdet.

[4] Cisco, What is cyber resilience: https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-cyber-resilience.html

[5] NSM, Grunnprinsipper for IKT-sikkerhet: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt

SIKKERHET I NETTVERKS- OG INFORMASJONSSYSTEMER: NIS2-DIREKTIVET

NIS2-direktivet (The Network and Information Security Directive 2.0) skal heve minimumsnivået på sikkerhetsområdet i alle EUs medlemsland. NIS2 krever systematisk «due diligence», rapportering og ledelsesfokus – og gjør at nye arbeidsstrømmer må etableres i mange norske selskaper.

Norge er ikke medlem av EU, men direktivet vurderes som EØS-relevant. Inntil videre bør beslutningstakere i Norge følge direktivets minimumskrav, og følge Sveriges implementering og veiledninger for svenske virksomheter.

NIS2-direktivet- hva er nytt?

UTVIDET VIRKEOMRÅDE	Flere sektorer omfattes, og regler for virksomhetsstørrelse innføres for å sikre harmonisering mellom landene.
ØKTE SIKKERHETSKRAV	Direktivet fastsetter en minimumsstandard for sikkerhetstiltak og håndtering av hendelser for å heve det felles sikkerhetsnivået. Medlemslandene kan beslutte tillegg eller skjerpede krav, men direktivet utgjør den grunnleggende standarden som skal implementeres.
SANKSJONER	For virksomheter som ikke overholder regelverket, kan sanksjoner pålegges på opptil 10 millioner EUR eller 2 prosent av den globale årsomsetningen.
SIKKERHETSKRAV I LEVERANDØRKJEDEN	For å håndtere den økende tredjepartsrisikoen, utvides sikkerhetskravene til også å omfatte virksomhetens leverandørkjede.
ØKTE KRAV TIL LEDELSEN	De styrende organene i virksomhetene er ansvarlige for å godkjenne sikkerhetstiltakene og overvåke implementeringen av disse, og kan også holdes ansvarlige ved manglende overholdelse. Ledelsen må gjennomgå opplæring for å kunne identifisere risikoer og vurdere risikostyringstiltakene og deres innvirkning på tjenestene som virksomheten leverer.
ØKT KRAV TIL RAPPORTERING	Hver medlemsstat skal sikre at vesentlige og viktige enheter uten unødig forsinkelse informerer sitt CSIRT-enhets eller, når det er aktuelt, sitt kompetente organ i samsvar med punkt 4 om alle hendelser som har en betydelig innvirkning på leveringen av deres tjenester i henhold til punkt 3 (betydelig hendelse). Når det er hensiktsmessig, skal berørte enheter uten unødig forsinkelse informere mottakerne av deres tjenester om betydelige hendelser som sannsynligvis vil påvirke leveringen av tjenestene negativt.

Sverige har nylig levert en første offentlig delutredning som har vurdert hvordan direktivet skal reguleres i svensk lov.

NIS2-direktivet er en del av en større pakke med tiltak fra EU, hvor også direktiv (EU) 2022/2557 om kritiske enheters motstandsdyktighet (CER-direktivet) inngår. NIS2-direktivet følger samme tidsplan og skal implementeres sammen med det såkalte CER-direktivet (direktiv for styrket motstandskraft i samfunnskritisk virksomhet). For berørte virksomheter er det fornuftig å **arbeide med begge direktivene parallelt**.

I den svenske utredningen foreslås nye regler om cybersikkerhet (SOU 2024:18), og inneholder:

- Krav om meldeplikt, risikohåndteringsforanstaltninger og hendelsesrapportering for virksomhetsutøvere som omfattes av reguleringen.
- Identifisering av hvilke myndigheter som skal utøve tilsyn i henhold til den nye reguleringen, og hvilke funksjoner som skal være hos Myndigheten for samfunnssikkerhet og beredskap.
- Økte muligheter for tilsynsmyndigheten til å vedta sanksjoner og økte sanksjonsgebyrer hvis en virksomhetsutøver bryter med reguleringen.

Utredningen foreslår at bestemmelsene skal tre i kraft i Sverige fra 1. januar 2025. [6]

SVENSKE KOMMUNER OG FYLKESKOMMUNER OMFATTES OGSÅ AV NIS2

[6] Regeringen, SOU 2024: 18: https://www.regeringen.se/contentassets/1e56bf5cad214fc78eb80d91c11cccb6/nya-regler-om-cybersakerhet-sou-202418.pdf

Utredningen foreslår at Sveriges nye cybersikkerhetslov som skal gjennomføre direktivet i Sverige, skal gjelde for de fleste statlige myndigheter i Sverige. Alle regioner og kommuner er også omfattet av lovens krav. Utredningen foreslår også at utdanningsinstitusjoner med eksamenstillatelse skal omfattes. Dette blir en **ny virkelighet for alle kommuner og fylkeskommuner, og høyskoler/læresteder i Sverige**. Det kan bli en lignende innføring i Norge. Beslutningstakere i Norge, både innenfor offentlig forvaltning, kommune- og fylkeskommuner/regioner og høyskoler/universiteter bør forberede seg på å tilfredsstille minimumskravene og investere i økt motstandskraft. [7]

Tilbydere av samfunnsviktige tjenester innen 18 definerte sektorer omfattes. Alle virksomheter av en viss størrelse og en viss type skal være omfattet. Også mindre virksomheter som anses å ha en nøkkelrolle for samfunnet, omfattes av direktivet. Tilbydere deles inn i tilbydere av **vesentlige** tjenester og tilbydere av **viktige** tjenester. Der sektorspesifikke regler, som kraftberedskapsforskriften, har strengere minimumsregler enn NIS 2, skal det sektorspesifikke regelverket gjelde.

Denne sjekklisten gir en oversikt over hvilke virksomheter som er omfattet:

SJEKKLISTE: VIL DIN VIRKSOMHET BLI OMFATTET AV KOMMENDE NIS2-REGLER?

Vesentlig eller viktig virksomhet	Følgende vesentlige virksomheter er definert som omfattet i direktivet: **1. energi** 2. transport 3. bank 4. finansmarkedsinfrastrukturer 5. helse 6. drikkevann 7. avløpsvann 8. digital infrastruktur 9. IKT-tjenester 10. offentlig forvaltning (sentral og regional) og 11. romvirksomhet.	Følgende viktige virksomheter er definert som omfattet i direktivet: 1. post- og kurertjenester 2. avfallshåndtering 3. produksjon og distribusjon av kjemikalier **4. matproduksjon** 5. produksjon av visse varer (medisinsk utstyr, IKT-utstyr, kjøretøy, elektronikk, maskiner og transportutstyr) 6. tilbydere av digitale tjenester og 7. forskning.
Vilkår	**To vilkår, som begge må være oppfylt. Se under:**	
Vilkår 1 Bedriftsstørrelse	**Direktivet omfatter kun bedrifter som er over en viss størrelse. Definisjonen følger av EU-direktiv** 2003/361/EC, og innebærer at følgende bedrifter er omfattet: Antall ansatte: Over 50	
Vilkår 2 Årlig omsetning	**Direktivet omfatter kun bedrifter som er over en viss størrelse. Definisjonen følger av EU-direktiv** 2003/361/EC, og innebærer at følgende bedrifter er omfattet: **Årlig omsetning: Over 114 millioner kroner (10 millioner EURO)**	

[7] Regeringen, SOU 2024:18: https://www.regeringen.se/contentassets/1e56bf5cad214fc78eb80d91c11cccb6/nya-regler-om-cybersakerhet-sou-202418.pdf

VIKTIGE UNNTAK- SOM ER OMFATTET UANSETT STØRRELSE OG OMSETNING

Viktige unntak fra ovennevnte regler, er at **uavhengig av størrelsen på virksomhet**, vil den gjelde din type virksomhet innen energisektoren, dersom du oppfyller kriteriene i bilag 1 eller 2:

	DELSEKTOR	TYPE AV VIRKSOMHET
SEKTOR: ENERGI	a) Elektrisitet	El-selskaper i henhold til definisjonen i artikkel 2.57 i Europaparlamentets og rådets direktiv (EU) 2019/944 (1), som driver leveranser i henhold til definisjonen i artikkel 2.12 i nevnte direktiv.
		Systemansvarlige for distribusjonssystemer i henhold til definisjonen i artikkel 2.29 i direktiv (EU) 2019/94
		Systemansvarlige for overføringssystemer i henhold til definisjonen i artikkel 2.35 i direktiv (EU) 2019/944
		Produsenter i henhold til definisjonen i artikkel 2.38 i direktiv (EU) 2019/944
		-Utpekte elektrisitetsmarkedsoperatører i henhold til definisjonen i artikkel 2.8 i Europaparlamentets og Rådets forordning (EU) 2019/943[8] - Markedsaktører i henhold til definisjonen i artikkel 2.25 i forordning (EU) 2019/943, og som tilbyr aggregering, etterspørselsfleksibilitet eller energilagringstjenester i henhold til definisjonen i artikkel 2.18, 2.20 og 2.59 i direktiv (EU) 2019/944 -Ladeoperatører som har ansvar for administrasjon og drift av et ladepunkt og som tilbyr en ladetjeneste til sluttbrukere, selv når dette utføres på vegne av en mobilitetstjenesteleverandør og i dennes navn.
	b) Fjernvarme eller fjernkjøling	Operatører av fjernvarme eller fjernkjøling i henhold til definisjonen i artikkel 2.19 i Europaparlamentets og Rådets direktiv (EU) 2018/2001[9]
	c) Olje	-Operatører av oljeledninger -Operatører av oljeproduksjonsanlegg, raffinerier, bearbeidingsanlegg og anlegg for lagring og overføring av olje -Sentrale lagringsenheter i henhold til definisjonen i artikkel 2 f i Rådets direktiv 2009/119/EF[10]
	d) Gass	-Leveransevirksomheter i henhold til definisjonen i artikkel 2.8 i Europaparlamentets og Rådets direktiv 2009/73/EF - Systemansvarlige for distribusjonssystemet i henhold til definisjonen i artikkel 2.6 i direktiv 2009/73/EF - Systemansvarlige for overføringssystemet i henhold til definisjonen i artikkel 2.4 i direktiv 2009/73/EF

[8] Europaparlamentets og Rådets forordning (EU) 2019/943 av 5. juni 2019 om det indre markedet for elektrisitet (EUT L 158, 14.6.2019, s. 54).

[9] Europaparlamentets og Rådets direktiv (EU) 2018/2001 av 11. desember 2018 om fremme av bruken av energi fra fornybare energikilder (EUT L 328, 21.12.2018, s. 82)

[10] Rådets direktiv 2009/119/EF av 14. september 2009 om plikt for medlemsstatene til å ha minimumslagre av råolje og/eller petroleumsprodukter (EUT L 265, 9.10.2009, s. 9)

		- Systemansvarlige for lagringssystemet i henhold til definisjonen i artikkel 2.10 i direktiv 2009/73/EF. -Systemansvarlige for en LNG-anlegg i henhold til definisjonen i artikkel 2.12 i direktiv 2009/73/EF. -Naturgasselskaper i henhold til definisjonen i artikkel 2.1 i direktiv 2009/73/EF - Operatører av raffinerier og bearbeidingsanlegg for naturgass
	e) Hydrogen	Operatører av anlegg for produksjon, lagring og overføring av hydrogen

STYRKING AV SIKKERHETSKRAV

NIS2-direktivets artikkel 21 pålegger medlemsstatene å sikre at tilbydere iverksetter hensiktsmessige og proporsjonale tekniske og organisatoriske tiltak for å håndtere **risiko i nettverk og informasjonssystemer**, slik som etter gjeldende NIS-direktiv.

STYRKEDE KRAV TIL LEDELSE

Artikkel 20 i direktivet omtaler spesielt **krav til Ledelse** av risikostyringen og det er tydelige krav til hvordan de omfattede virksomhetene skal operere:

1. Medlemsstatene skal sikre at **ledelsesorganene i vesentlige og viktige enheter godkjenner cybersikkerhetstiltakene** som disse enhetene iverksetter for å følge artikkel 21, overvåker gjennomføringen av dem, og kan holdes ansvarlige for enhetenes brudd på denne artikkelen.
2. Medlemsstatene skal sikre at medlemmene i vesentlige og viktige enheters ledelsesorgan er **forpliktet til å gjennomgå opplæring**, og skal oppmuntre vesentlige og viktige enheter til **jevnlig å tilby lignende opplæring til sine ansatte**, slik at de får tilstrekkelig kunnskap og kompetanse til å identifisere risikoer og vurdere risikostyringspraksis for cybersikkerhet og deres påvirkning på tjenestene som tilbys av enheten.

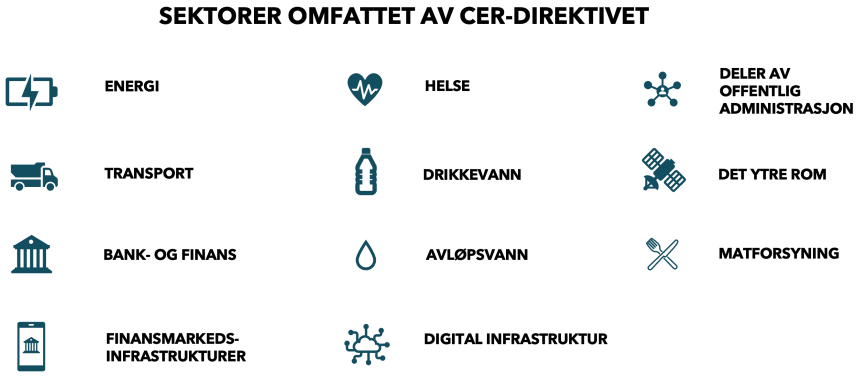
I artikkel 21 i direktivet står selve tiltakene for risikohåndtering for cybersikkerhet som kreves av omfattede virksomheter. Vi har laget en oversikt over minimumslisten nedenfor:

NIS2: RISIKOSTYRINGSMETODE MED EN MINIMUMSLISTE OVER GRUNNLEGGENDE SIKKERHETSELEMENTER

Illustrasjon av minimumslisten av grunnleggende sikkerhetselementer i henhold til NIS 2, artikkel 21. Kilde: Radar Norway

CER-DIREKTIVET

Ifølge CER-direktivet skal medlemsstatene sikre evnen til samfunnskritisk virksomhet til å forebygge, motstå og håndtere forstyrrelser eller avbrudd i virksomheten. Dette skal gjelde uavhengig av om forstyrrelsen eller avbruddet har blitt forårsaket av for eksempel naturkatastrofer, terrorangrep, pandemier eller andre alvorlige hendelser.
Direktivet gjelder ikke forhold som er dekket av NIS2-direktivet. Bestemmelsene i direktivet gjelder heller ikke der det i EU-sektorregelverk stilles tilsvarende krav til kritiske enheters motstandsdyktighet.



Sektorer omfattet av CER-direktivet. Kilde: Radar Norway, 2024.

CER-direktivet forplikter medlemsstatene til å identifisere aktører (såkalte **kritiske enheter**) som tilbyr samfunnskritiske tjenester innen sektorene energi, transport, bankvirksomhet, finansmarkedets infrastruktur, helsevesen, drikkevann, avløpsvann, digital infrastruktur, offentlig forvaltning, rommet samt produksjon, bearbeiding og distribusjon av matvarer. Direktivet pålegger de kritiske enhetene plikter, blant annet å **styrke sin motstandsdyktighet** og **rapportere hendelser**. Det inneholder også bestemmelser om tilsyn og sanksjoner.
For å sikre samsvar mellom de to direktivene, forskrives det i disse at enheter som er identifisert som kritiske enheter i henhold til CER også skal anses å være vesentlige enheter i henhold til NIS2.

CYBER RESILIENCE ACT- CYBERMOTSTANDSDIREKTIVET

Cybermotstandsdirektivet er en kommende forordning om regulering av krav til cybersikkerhet i produkter med digitale elementer og software. Produkter som dekkes av forslaget er bredt og vil gjelde alt fra eksempelvis smartklokker og leketøy til rutere og brannmurer samt programvare som benyttes i produktene. Produkter som dekkes av rettsakten må være bygget slik at de ivaretar kravene til cybersikkerhet. Reglene fastsetter[11]:

a) regler for markedsføring av produkter med digitale elementer for å sikre produktenes nettsikkerhet,
b) krav til design, utvikling og produksjon av produkter med digitale elementer, og forpliktelser for virksomhetene knyttet til disse produktene,
c) krav til sårbarhetshåndteringsprosessene som produsentene skal innføre for å sikre cybersikkerheten til produkter med digitale elementer gjennom hele livssyklusen, og

[11] Posisjonsnotat EØS-notatbasen: https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2022/juni/cyber-resilience-act/id2984059/

forpliktelser for virksomhetene i disse prosessene. Produsentene vil også måtte rapportere aktivt utnyttede sårbarheter og hendelser,

d) regler om markedsovervåking og håndheving

CYBER SECURITY ACT- CYBERSIKKERHETSLOVEN OG TILHØRENDE FORORDNING

Forordningen innebærer at EUs cybersikkerhetsbyrå ENISA får et styrket budsjett, flere ansatte og et styrket og permanent mandat og vil dermed spille en større rolle i EUs cybersikkerhetslandskap. Forordningen etablerer også et felleseuropeisk rammeverk for frivillig sertifisering av IKT-produkter, tjenester og prosesser.

Forordningen etablerer også et felleseuropeisk rammeverk for frivillig sertifisering av IKT-produkter, tjenester og prosesser (Definert i artikkel 2 nr. 12,13 og 14). Forordningen setter i denne sammenheng også et krav om at medlemslandene skal etablere tilsynsmyndigheter og andre roller for sikkerhetssertifisering. Cybersikkerhetsforordningen er tatt inn i EØS-retten, med forbehold om godkjennelse.[12]

OPPSUMMERING EUROPEISKE REGLER OG KRAV SOM PÅVIRKER NORGE

Et stort antall norske og europeiske regler kommer på løpende bånd fremover. En fellesnevner for å møte endringene som kommer, er **økte krav til kompetanse om risiko og økt ledelsesansvar for økt motstandskraft i virksomheter.**

NIS2-direktivet gjør at omfattede virksomheter må gjøre tiltak for å håndtere **risiko i nettverk og informasjonssystemer.** Det kreves en risikostyringsmetode med en minimumsliste over grunnleggende sikkerhetselementer, blant annet krav om at tilbydere håndterer cybersikkerhetsrisiko i f**orsyningskjeder** og hos **leverandører**, og det kommer **sterkere krav til ledelse**. Offentlige myndigheter omfattes, og beslutningstakere i det offentlige Norgenbør derfor også forberede seg på å tilfredsstille minimumskravene og investere i økt motstandskraft.

CER-direktivet forplikter medlemsstatene til å identifisere aktører (såkalte **kritiske enheter**) som tilbyr samfunnskritiske tjenester innen sektorene energi, transport, bankvirksomhet, finansmarkedets infrastruktur, helsevesen, drikkevann, avløpsvann, digital infrastruktur, offentlig forvaltning, rommet samt produksjon, bearbeiding og distribusjon av matvarer. De kritiske enhetene får nye plikter, blant annet å **styrke sin motstandsdyktighet** og **rapportere hendelser**.

Cybermotstandsdirektivet skal **redusere sårbarheter i produkter** i EU/EØS, og sikre at produsenter blir ansvarlige for cybersikkerheten i produktene gjennom hele produktets livssyklus. produkter som dekkes av rettsakten må være bygget slik at de ivaretar kravene til cybersikkerhet. Dette vil innebære økte kostnader for produsenter, og samtidig mulighet for innkjøpere av produktene til å styrke virksomhetenes motstandskraft gjennom innkjøp av pålitelige produkter.

Gjennomgangen av både det geopolitiske, økonomiske, trusselsituasjonen og det regulatoriske bildet viser at norske beslutningstakere møter et **økt trusselnivå, økte kostnader og økte regulatoriske og administrative krav**. I tillegg til de europeiske reglene, som vil gjennomføres i norsk rett i flere tilfeller, må beslutningstakerne også tilfredsstille strenge reguleringer gjennom eksisterende norske lover og forskrifter på sikkerhet- og beredskapsområdet.

[12] Europalov, Cybersikkerhetsforordningen: https://europalov.no/rettsakt/cybersikkerhetsforordningen/id-10405

DYPDYKK I BRANSJENE KRAFT- OG ENERGI OG MAT- OG PROSESSERING

I denne rapporten dypdykker vi inn i to sektorer som er viktige for Norge: Kraft- og energisektoren og mat- og prosesseringsindustrien. Begge sektorer har høy utbredelse av IT/OT- systemer, og har komplekse verdikjeder som utgjør sårbarheter som kan utnyttes. Kraft- og energisektoren har imidlertid kommet lengre enn mange andre sektorer hva gjelder digital modenhet, og er også spesifikt nevnt som essensiell og viktig sektor i de nye europeiske reguleringene NIS2- og CER-direktivet.

Tilsynsregimet og regelverksutviklingen er derimot ulik for de to sektorene. Mat- og prosesseringsindustrien har i motsetning til kraftsektoren ikke tidligere hatt et strengt regelverk på IKT-sikkerhet, men blir fremover omfattet av nye regler som CER-direktivet og NIS2-direktivet.

Vi har derfor valgt å belyse nærmere hvilke utfordringer og muligheter som gjelder for de to sektorene. Til slutt oppsummerer vi bransjegjennomgangen, og kommer med anbefalinger til de utvalgte bransjene, men også generelle anbefalinger som gjelder på tvers av sektorer.

Vi vil nå belyse de spesifikke kravene, nåsituasjonen på IKT-sikkerhet og anbefalinger til beslutningstakere som gjelder i en av sektorene som er definert som essensiell sektor i NIS2-direktivet; nærmere bestemt kraft- og energisektoren.

BRANSJEPERSPEKTIV PÅ MOTSTANDSKRAFT: KRAFT- OG ENERGIBRANSJEN

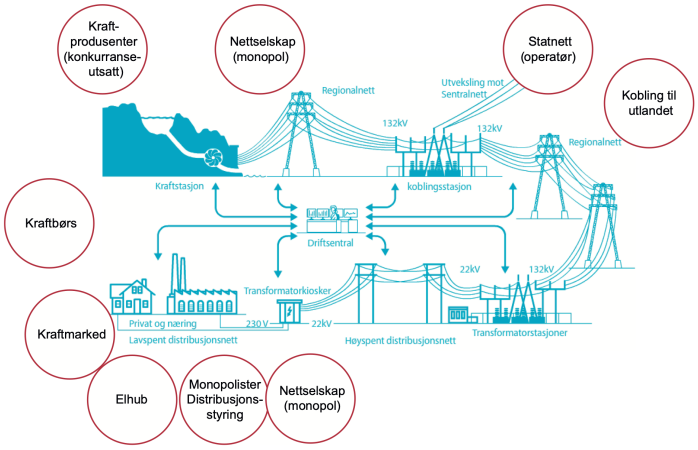
Vi gir først en analyse av nåsituasjonen for utviklingen, modenheten og IKT-sikkerheten i bransjen, før vi gjennomgår nasjonale lover og regler som påvirker beslutningstakerne i kraftsektoren. Til slutt i bransjegjennomgangen gir vi noen anbefalinger på hva beslutningstakere i bransjen nå bør gjøre for å styrke sin motstandskraft og sikkerhet.

STORSTILT OMSTILLING I KRAFT- OG ENERGISEKTOREN

Den europeiske kraftsektoren gjennomgår en storstilt omstilling, både grunnet klimaforpliktelser og behovet for å redusere avhengigheten av russisk naturgass. [13] Kraftforsyningen eier og driver en av Norges mest **samfunnskritiske infrastrukturer**. Både myndighetene og ledelse i virksomheter har derfor høyt fokus på informasjonssikkerhet, et forhold som nett- og produksjonsselskapene må forholde seg til på en forsvarlig og hensiktsmessig måte.

Som vist på figuren, er kraftsystemet et sammenhengende og komplekst system.

[13] Forsvarets forskningsinstitutt, 23/02425: https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/3241/23-02425.pdf



Det norske kraftsystemet. Hentet fra NOU 2015:13. [14]

Kraftnettet deles inn i tre nettnivåer: sentral-, regional- og distribusjonsnett. Sentralnettet knytter sammen forbrukere, produsenter og overføringsledninger til utlandet, Regionalnettene er bindeledd mellom sentralnettet og distribusjonsnettene. Distribusjonsnettene sørger normalt for distribusjon av kraft til sluttbrukerne, som husholdninger, tjenesteytere og annen næringsvirksomhet.

Sentralnettet drives som en enhet med Statnett SF som operatør og dominerende eier (om lag 90 prosent). Det øvrige sentralnettet er fordelt mellom 20 eiere. Underliggende nett har en variert eiersammensetning. Det er mange nettselskaper, og enkelte selskaper eier både deler av sentralnettet og regionalnett. Noen få av dem eier også distribusjonsnett.

DIGITAL MODENHET I KRAFT- OG ENERGISEKTOREN

Fremtidens «smarte» kraftsystem preges av økt produksjon fra fornybare energikilder og krav til forbrukerfleksibilitet som øker. Overvåking og drifting av nettet vil i økende grad skje gjennom **digitalisering og automatiserte prosesser**. Mye av teknologiutviklingen i kraftbransjen er knyttet til ny og endret bruk av sensorer og informasjon fra disse. Dette omtales gjerne som **tingenes internett** (Internet of Things – IoT) og industriens tingenes internett (Industrial Internet of Things - IIoT).

IT, OT OG TINGENES INTERNETT

Begreper som ofte nevnes innen IKT-sikkerhet, er IT, OT og tingenes internett. Disse defineres nedenfor.

IT- Informasjonsteknologi- er et begrep som omfatter teknologi for innsamling, lagring, behandling, overføring og presentasjon av informasjon. I NVEs nye veileder er informasjonsteknologi definert slik[15]:

> «(IT) omfatter systemer, maskinvare, programvare og nettverk som brukes til databehandling, datalagring og kommunikasjon innenfor en organisasjon. IT handler om å administrere og sikre digital informasjon, støtte forretningsdriften og legge til rette for kommunikasjon og samarbeid mellom brukere. Vanlige IT-funksjoner inkluderer administrasjon av servere, databaser, cybersikkerhet, programvareutvikling og teknisk brukerstøtte.»

Kilde: NVE, Rettleiar for vurdering av digital risiko, 2024

[14] NOU 2015:13, https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

[15] NVE, Rettleiar for vurdering av digital risiko: https://publikasjoner.nve.no/veileder/2024/veileder2024_02.pdf

OT –Operasjonell teknologi- omfatter maskinvare- og programvaresystemene som brukes til å overvåke, kontrollere og administrere fysiske prosesser i ulike bransjer og i kritisk infrastruktur. NVE definerer i sin nye veileder OT på følgende måte:

> «Operasjonell teknologi (OT) refererer til spesialisert maskinvare og programvare som brukes til å overvåke og kontrollere fysiske prosesser og enheter i industrielle omgivelser som produksjonsanlegg, kraftverk og transportsystem. OT-systemer er designet for å administrere og optimalisere prosesser i sanntid, og involverer ofte sensorer, aktuatorer og industrielle kontrollsystemer. OT i form av driftskontrollsystemer spiller en avgjørende rolle i styringen av kraftforsyningen, og sikrer sikkerhet, effektivitet og pålitelighet av kraftproduksjon og drift av nettet.»

Kilde: NVE, Rettleiar for vurdering av digital risiko, 2024

Driftskontrollsystemer er operasjonell teknologi som er avhengig av IT for å kunne levere. NVE definerer Tingenes internett slik[16]:

> «**Tingenes internett (IoT)** beskriver et nettverk av fysiske enheter som kobles sammen, og samler informasjon som deles med hverandre via internett. Det inkluderer hardware (sensorene), overførings- og kommunikasjonsløsning (EDGE, 4G o.l.), og lagring av informasjonen (skyløsning). I tillegg inkluderes ofte også analysene og tolkningen av informasjonen (Big data) i dette begrepet.»

DIGITALE SÅRBARHETER OG RISIKO I KRAFTFORSYNINGEN

Digitaliseringsprosessene i kraftsektoren gjør at flere sentrale funksjoner i dag støttes av IKT-løsninger som integreres i systemene og mellom systemene. Konsekvensen er lange digitale verdikjeder med komplekse samhandlingsmønstre og avhengighetsforhold, noe som bidrar til økt kompleksitet i kraftbransjen. Sårbarheter kan oppstå i alle ledd, forplante seg videre i verdikjeden, og gjøre bransjen mer utsatt for cybertrusler (NOU 2015:13, 2015).

Digitalisering treffer kraftbransjen gjennom digitale sensorer i infrastrukturen, skytjenester og utsetting av IT-drift og gjennom avanserte måle- og styringssystemer (AMS). IKT er i dag en integrert og svært viktig del av energiforsyningen for effektiv drifts- og forsyningssikkerhet. Ifølge Utvalget om digitale sårbarheter har driftskontrollsystemene derfor blitt knyttet stadig tettere opp mot tilgrensende systemer som for eksempel systemer for måling, avregning og fakturering, kundeinformasjonssystemer (KIS), nettinformasjonssystemer (NIS), geografiske informasjonssystemer (GIS) og kontorstøttesystemer.

Virksomheter i kraftforsyningen har sterk avhengighet av leverandører på området IKT-sikkerhet og IT- drift. Mens Norges vassdrags- og energidirektorat (NVE) setter krav til virksomhetene gjennom kraftberedskapsforskriften, er det virksomhetene selv som skal inngå sikkerhetsavtale med leverandørene og følge opp at leverandørene leverer tjenester i henhold til kravene i kraftberedskapsforskriften.

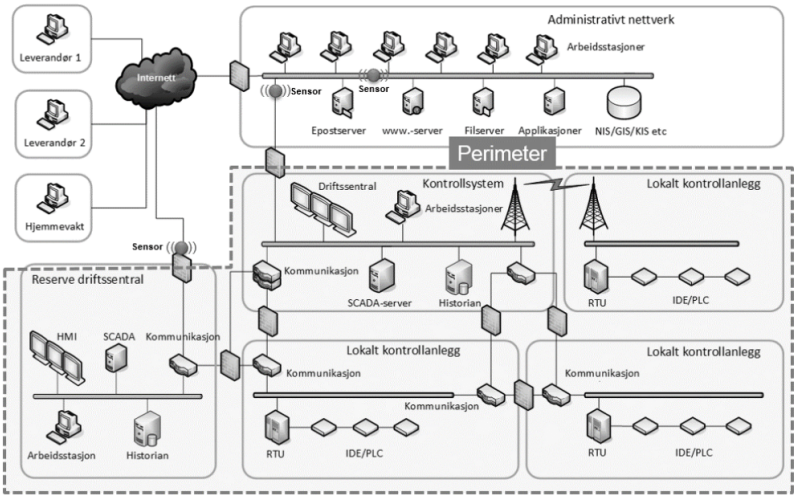
[16] NVE, Eksternrapport 2020/02: https://publikasjoner.nve.no/eksternrapport/2020/eksternrapport2020_02.pdf

Energibransjen har gjennom mange år benyttet seg av IKT-systemer for å støtte driften, overvåke og fjernstyre anleggene i energiforsyningen. Systemene er svært komplekse, og inkluderer driftskontrollsystemet (SCADA), datanettverk for signaloverføring til og fra SCADA-systemet og ut til anleggene, stasjonsdatamaskiner og utstyr som konverterer digitale signaler til fysisk handling i stasjonene, samt nettverksutstyr som knytter driftskontrollsystemet sammen. Driftssentralene er også inkludert i driftskontrollsystemet, der operatørene mottar sanntidsinformasjon om kraftsystemets tilstand og kan fjernstyre anleggene. Tidligere var disse systemene helt unike og uavhengige av andre IKT-systemer som virksomhetene brukte. De ble utviklet med fokus på maksimal tilgjengelighet og integritet, mens konfidensialitet ikke var en prioritet, da systemene ikke hadde kontakt med omverdenen. I dag er situasjonen helt annerledes.[17]

Flere av respondentene i NVEs rapport fra 2023 nevnte mulig risiko knyttet til digitalisering og automatisering av driftskontrollsystemene (OT). Denne automatiseringen vil ha betydning for beredskapen. Kraftberedskapsforskriften har strengere krav til sikring av driftskontrollsystemer enn til informasjonssikkerhet og digitale systemer. Dette fordi funksjonene til OT-systemene er kritiske for leveransen. Den økte digitale konvergensen kan gjøre det vanskeligere å se skillet mellom OT- og IKT-systemene, og dermed gjøre det mer utfordrende å avgjøre hvilken del av forskriften som skal følges.

Digitaliseringen gjør at grensene for hva som er OT flytter seg, og konvergensen mellom IKT og OT øker. Modenheten av IKT-sikkerhet er lavere innen OT, og det kan skape utfordringer fremover.
I takt med at industrielle operasjoner digitaliseres, trenger OT-ressurser og industrielle nettverk en **solid IT-infrastruktur** for å muliggjøre oppetid og hjelpe til med å øke hastigheten på industrielle prosesser for å øke produksjonen. Mer enn noen gang må IT- og OT-team samarbeide for å implementere en moderne, administrert, smidig og sikker kablet og trådløs nettverksinfrastruktur som vil bidra til å øke industriell produktivitet og redusere driftskostnadene.

NVE har en god illustrasjon på det komplekse systemet for driftskontroll i kraftforsyningen:



Driftskontrollsystem og administrativt nettverk. Alt innenfor stiplet linje regnes som driftskontrollsystem (Kilde NVE Veiledning 2013).

Figuren viser hvorfor IKT er en viktig del av energiforsyningen, samt hvorfor de komplekse systemene også utgjør digitale sårbarheter som kan utnyttes- og derfor må beskyttes.

[17] NOU 2015:13: https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/?ch=4#kap13

1. januar 2019 ble NVE utpekt som sektorvist responsmiljø for å koordinere og håndtere IKT-sikkerhetshendelser i kraftforsyningen. Fra 2019 har også KraftCERT AS utført visse oppgaver innen varsling, informasjonsdeling og analyse av IKT-sikkerhetshendelser for å støtte NVE som sektorvist responsmiljø. KraftCERT ble opprettet av store aktører i kraftforsyningen i 2014 for å hjelpe medlemsselskapene med å forebygge og håndtere IKT-sikkerhetshendelser. [18]

Den norske kraftsektoren er, fordi den er samfunnskritisk og sårbar, omfattet av en rekke nasjonale lover og forskrifter, som vi gjennomgår nedenfor.

NASJONALE LOVER OG REGLER SOM PÅVIRKER KRAFTSEKTOREN

Energiloven, sikkerhetsloven og kraftberedskapsforskriften har regler som bidrar til at Norge har god leveringssikkerhet på elektrisitet og god beredskap i ekstraordinære situasjoner. NVE fører beredskapstilsyn etter både kraftberedskapsforskriften og energilovforskriften. I tillegg fører de tilsyn etter sikkerhetsloven og kraftrasjoneringsforskriften.

NVE anser at det ikke er noen myndighet i noen andre land som har tilsvarende regelverk som Norge for beskyttelse av driftskontrollsystemer, men innen Norden ser de at særlig Finland er spesielt kompetent på IKT-sikkerhet i flere sektorer, også energiforsyningen. Selv om Norge har flere lover og forskrifter som skal sikre Norges beredskap og sikkerhet, finnes det digitale sårbarheter i kraftforsyningen som kan utnyttes. Et sterkt og strengt regelverk alene er ikke nok til å styrke motstandskraften hos virksomhetene i kraftsektoren. Faktisk etterlevelse av funksjonskravene i regelverket krever et **ordentlig, systematisk og risikobasert sikkerhetsarbeid**.

Energiloven og beredskapsforskriften regulerer sikkerhet og beredskap i kraftsystemet, herunder informasjonssikkerhet. Beredskap i kraftforsyningen reguleres i kraftberedskapsforskriften. Beredskapsforskriften omfatter krav om organiseringen av en egen beredskapsorganisasjon, Kraftforsyningens Beredskapsorganisasjon (KBO). KBO setter strukturen for samordning og ledelse av kraftforsyningen, og skal effektivt kunne håndtere og forebygge hendelser i kraftforsyningen.

KBO består av NVE, Statnett og større kraftprodusenter, nettselskaper og fjernvarmeselskaper som har anlegg med vesentlig betydning for drift eller gjenoppretting av produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme.

Bestemmelsene omfatter både forebyggende, skadebegrensende og beredskapsmessige tiltak. Beredskapsforskriften skal sikre at energiforsyningen opprettholdes, og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere samfunnsmessige konsekvenser av strømutfall. Beredskapsforskriften stiller strenge krav til risikovurderinger, tilgangskontroll og tilgang til systemene fra leverandører. I tillegg er kravene i forskriften differensiert, slik at de viktigste selskapene er underlagt de strengeste sikkerhetskravene. Nedenfor gjennomgår vi de viktigste reglene som angår motstandskraft for virksomheter i kraftsektoren, herunder energiloven, sikkerhetsloven og kraftberedskapsforskriften.

ENERGILOVEN

Kraftforsyningen i Norge er regulert gjennom energiloven. I lovens § 4-10, jf. § 4-8 fremgår reglene om sertifisering som operatør av transmisjonssystem (TSO).

[18] KraftCERT, https://www.kraftcert.no/no/#om

TSO står for Transmission System Operator, og er navnet på den som er systemansvarlig i det norske kraftsystemet. Systemansvarlig koordinerer driften av kraftsystemet, sørger for fastsettelse av kapasitet til markedet, håndterer flaskehalser og handler med andre land. I Norge har Statnett denne rollen.

I Energilovens kapittel 9 er kravene til beredskap omtalt.

ENERGILOVEN	
§9.1	**Kraftforsyningens beredskapsorganisasjon** Utdrag: *Kraftforsyningens beredskapsorganisasjon (KBO) består av de enheter som eier eller driver anlegg eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme.*
§9.2	**Beredskapstiltak** Utdrag: Den som helt eller delvis eier eller driver anlegg eller system som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme, plikter å sørge for **effektiv sikring og beredskap** og iverksette tiltak for å forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner som nevnt i § 9-1 fjerde eller femte ledd og for å gjenopprette normal situasjon.
§9.3	**Informasjonssikkerhet** Utdrag: Alle enheter i KBO skal vurdere sikkerheten ved all behandling av informasjon om kraftforsyningen. Enhetene skal kartlegge hvilken informasjon som er sensitiv, hvor den befinner seg og hvem som har tilgang til den. Det skal etableres effektiv avskjerming og beskyttelse av sensitiv informasjon. Enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen.

SIKKERHETSLOVEN

Sikkerhetsloven skal bidra til å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser. Den skal også bidra til å forebygge, avdekke og motvirke sikkerhetstruende virksomhet.[19]Sikkerhetsloven gjelder for virksomheter som spiller en særlig viktig rolle for opprettholdelsen av sentrale samfunnsfunksjoner, slik som for eksempel elektronisk kommunikasjon, helse, **kraftforsyning**, transport, vannforsyning, bank og finans, politi, forsvar og regjering.

Under følger en gjennomgang av de viktigste kravene til forebyggende sikkerhet.

SIKKERHETSLOVEN	
§4.1	**Sikkerhetsstyring** Virksomhetens leder har ansvaret for det forebyggende sikkerhetsarbeidet. Forebyggende sikkerhetsarbeid skal være en del av virksomhetens styringssystem. Sikkerhetstilstanden i virksomheten skal regelmessig kontrolleres. Virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse.

[19] Sikkerhetsloven: https://lovdata.no/dokument/NL/lov/2018-06-01-24

§4.2	**Vurdering av risiko** Virksomheten skal regelmessig gjennomføre vurdering av risiko. Vurderingen skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak. Virksomheten skal som del av vurderingen kartlegge hvilke virksomheter den er avhengig av for å fungere som den skal. Vurderingen skal gjennomgås jevnlig og om nødvendig revideres.
§4.3	**Plikt til å gjennomføre sikkerhetstiltak og øvelser** Utdrag: Virksomheten skal gjennomføre de forebyggende sikkerhetstiltakene som må til for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet. Slike tiltak kan gjennomføres i sammenheng med andre forebyggende sikkerhetstiltak i virksomheten, så lenge kravene i denne loven oppfylles. Kostnadene ved et sikkerhetstiltak skal stå i et rimelig forhold til det som kan oppnås ved tiltaket. Virksomheten skal regelmessig gjennomføre øvelser for å vurdere effekten av iverksatte sikkerhetstiltak.
§4.4	**Krav til dokumentasjon** Virksomheten skal dokumentere vurderingen av risiko og de gjennomførte og planlagte sikkerhetstiltakene.
§4.5	**Varslingsplikt** Virksomheten skal straks varsle sikkerhetsmyndigheten og andre myndigheter som skal utføre tilsyn i medhold av § 3-1 andre ledd, dersom a., den har blitt rammet av sikkerhetstruende virksomhet b., det er begrunnet mistanke om at sikkerhetstruende virksomhet har rammet eller vil kunne ramme virksomheten eller andre virksomheter c., det har skjedd alvorlige brudd på krav til sikkerhet etter kapittel 5, 6 eller 7.

FORSKRIFT FOR SIKKERHET OG BEREDSKAP I KRAFTFORSYNINGEN

Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften), er hjemlet i Energiloven, kapittel 9 om beredskap. *Virksomheter og personell som faller innenfor energilovens og kraftberedskapsforskriftens virkeområde, plikter å oppfylle kravene som gjelder i både energiloven kapittel 9 og kraftberedskapsforskriften.*

Kraftberedskapsforskriften fastsetter krav og retningslinjer for å sikre sikkerhet og beredskap innen kraftforsyning i Norge. Forskriften omhandler tiltak og forpliktelser for aktører i kraftsektoren, inkludert kraftprodusenter, nettoperatører og andre relevante parter.

Forskriften skal sikre en pålitelig og trygg kraftforsyning, samt å håndtere situasjoner som kan true kraftsystemets stabilitet eller forsyningssikkerheten. Den omfatter krav til planlegging, risikovurdering, beredskapsforberedelser, øvelser og rapportering for å styrke sektorens evne til å håndtere ulike typer hendelser, fra tekniske feil til eksterne påvirkninger. Ved å følge forskriften for sikkerhet og beredskap i kraftforsyningen bidrar aktørene til å opprettholde et høyt sikkerhetsnivå og håndtere potensielle utfordringer i kraftsektoren, og dermed sikre en pålitelig strømforsyning til samfunnet.

Kravene i kraftberedskapsforskriften pålegger virksomheten plikter som må oppfylles mens virksomheten er i normal driftsituasjon og før det er oppstått en ekstraordinær situasjon. Pliktene kan

ivaretas ved å iverksette forebyggende sikringstiltak og planlegge og forberede beredskapstiltak. Videre pålegges virksomheten plikter underveis i og etter alle former for ekstraordinære situasjoner som kan skade eller hindre kraftforsyningen.

KRAFTBEREDSKAPSFORSKRIFTEN	
§1.4	**Lederansvar** «Leder for virksomhet som er omfattet av denne forskrift har ansvar for at virksomheten er organisert og har funksjoner og ressurser slik at virksomheten er innrettet for å oppfylle kravene i energiloven kapittel 9, energilovforskriften § 3-5 bokstav c, § 5-3 bokstav c, og at bestemmelser gitt i eller i medhold av denne forskrift oppfylles.» Fra NVEs veiledning til forskriften: Virksomhetens leder må kjenne til innholdet i energilovens kapittel 9 og kraftberedskapsforskriften, samt krav i energilovforskriften om beredskap. Leder for virksomheten kan være både daglig leder, styreleder, hele styret og/eller resten av toppledelsen. Det er virksomheten selv som er ansvarlig for å angi hvem som skal regnes som leder i virksomheten.
§1.5	**Beredskapsplikt og beredskapsplan** Virksomheter som er omfattet av denne forskrift skal sørge for effektiv sikring og beredskap, og skal iverksette tiltak for å forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner i samsvar med energiloven § 9-2 første ledd. Virksomheter som er omfattet av denne forskrift skal ha en beredskapsplan for å håndtere og begrense virkningene av ekstraordinære situasjoner.
§2.1	**Kraftforsyningens beredskapsorganisasjon** Med KBO menes kraftforsyningens beredskapsorganisasjon. KBO består av KBO-enhetene, KDS og beredskapsmyndigheten, samt KSL når denne trer i kraft, jf. § 3-3. Med KBO-enhet menes: a.De virksomheter som eier eller driver anlegg, system eller annet og som i medhold av § 5-2 eller § 5-7 er klassifisert etter denne forskrift. b. Andre virksomheter beredskapsmyndigheten har vedtatt er KBO-enhet i medhold av § 3-1 annet ledd. Med KDS menes kraftforsyningens distriktssjefer. Med KSL menes kraftforsyningens sentrale ledelse. Kraftforsyningens sentrale ledelse består av beredskapsmyndigheten med deltakelse fra Statnett SF. **Fra NVEs veiledning til forskriften:** Generelle krav for kraft- og beredskapsenheter: KBO-enheter er større kraftprodusenter, nettselskaper, fjernvarmeselskaper og større vindkraftverk som har klassifiserte anlegg.
§2.2	**Organisasjon og funksjon** KBO-enheter skal ha følgende funksjoner, som utpekes av leder for virksomheten: a) Beredskapsleder. Denne skal sørge for nødvendig planlegging og utøvelse av beredskapsarbeidet

	b) Beredskapskoordinator. Denne skal ha oversikt over beredskapsarbeidet i virksomheten og være administrativt kontaktpunkt til beredskapsmyndigheten c) IKT-sikkerhetskoordinator. Denne skal ha oversikt over IKT-sikkerhetsarbeidet i virksomheten og være faglig kontaktpunkt til beredskapsmyndigheten vedrørende IKT-sikkerhet **Fra NVEs veiledning til forskriften:** Effektiv beredskap krever klare ansvarslinjer. NVE betrakter funksjonene beredskapsleder, beredskapskoordinator og IKT-sikkerhetskoordinator som en del av virksomhetens kjernevirksomhet innenfor området beredskap. Funksjonene kan dermed ikke tjenesteutsettes eller deles mellom ulike virksomheter. Et unntak er i konsern der NVE har tillatt at konsernet innehar funksjonene beskrevet i § 2-2 på vegne av datterselskapene.
§2.3	**Risikovurdering** KBO-enheter skal gjennomføre risikovurdering knyttet til ekstraordinære forhold. Vurderingene skal ha et slikt omfang at enheten kan identifisere risiko og sårbarhet ved alle funksjoner, anlegg og tiltak av betydning for å oppfylle kravene i forskriften. Vurderingene skal minimum gjennomgås årlig og oppdateres ved behov.
§2.4	**Beredskapsplanlegging** KBO-enheter skal ha et oppdatert beredskapsplanverk tilpasset virksomhetens art og omfang. Planverket skal bygge på risikovurderinger og skal omfatte alle beredskapstiltak etter denne forskriften. Beredskapsplanleggingen skal blant annet omfatte forberedelser og tiltak det kan bli nødvendig å iverksette ved store ulykker, vesentlige skader, trusselsituasjoner, rasjonering og andre ekstraordinære situasjoner som kan påvirke kraftforsyningens drift og sikkerhet. Beredskapsplanverket skal, innenfor rammene av kapittel 6 om informasjonssikkerhet, samordnes med berørte myndigheter og andre relevante virksomheter, deriblant andre KBO-enheter.
§2.5	**Varsling** KBO-enheter skal uten ugrunnet opphold varsle beredskapsmyndigheten om ekstraordinære situasjoner. Situasjoner som angitt i § 2-6 bokstav a til h om rapportering, skal alltid varsles. Varselet skal kortfattet beskrive hendelsen, forventet gjenoppretting og kontaktperson.
§2.6	**Rapportering** KBO-enheter skal uten ugrunnet opphold og senest innen tre uker skriftlig innrapportere følgende uønskede hendelser til beredskapsmyndigheten: a. Forsøk på inntrengning og/eller manipulasjon av hele eller deler av driftskontrollsystemet og avanserte måle- og styringssystem (AMS). b. Innbrudd, hærverk, sabotasje eller andre kriminelle handlinger, eller forsøk på dette. c. Ved begrunnet mistanke om at sikkerhetstruende virksomhet har rammet eller vil kunne ramme virksomheten eller andre virksomheter. d. Situasjoner hvor kraftsensitiv informasjon er blitt kjent for andre enn rettmessige brukere, eller mistanke om dette. e. Avbrudd i distribusjon av elektrisitet i mer enn to timer som berører viktige samfunnsfunksjoner eller et stort antall sluttbrukere. f. Avbrudd i fjernvarmeforsyningen i mer enn 12 timer som berører viktige samfunnsfunksjoner eller et stort antall sluttbrukere. g. Større havarier i transmisjon- og regionalnettet.

	h. Omfattende feil og sikkerhetstruende hendelser i driftskontrollsystemer. Beredskapsmyndigheten kan kreve rapportering av andre tilfeller av uønskede hendelser enn de som er nevnt i første ledd. Beredskapsmyndigheten kan også pålegge virksomheter som eier eller driver anlegg eller system, som er eller kan bli av vesentlig betydning for produksjon, omforming, omsetning eller fordeling av elektrisk energi og fjernvarme, å rapportere uønskede hendelser i samsvar med annet ledd.
§2.7	**Øvelser** KBO-enheter skal gjennomføre øvelser med slikt innhold og omfang at enheten vedlikeholder og utvikler sin kompetanse til å håndtere alle aktuelle ekstraordinære situasjoner. Virksomheter skal ha en flerårig øvelsesplan og gjennomføre minimum én årlig øvelse.
§2.8	**Informasjonsberedskap** KBO-enheter skal ha en informasjonsplan og en effektiv informasjonsberedskap i ekstraordinære situasjoner. Dette skal blant annet omfatte informasjon internt i enheten, til berørte myndigheter, samfunnskritiske virksomheter, andre relevante KBO-enheter, publikum og media, samt råd til kunder. Informasjonsplanen skal inngå som del av beredskapsplanverket, øves jevnlig og evalueres.
§2.9	**Evaluering** KBO-enheter skal etter ekstraordinære situasjoner og øvelser gjennomføre en evaluering. Evalueringen skal brukes som grunnlag for at virksomhetens beredskapskompetanse utvikles, at risikovurderinger og beredskapsplaner oppdateres, og at det gjennomføres konkrete beredskapstiltak for anlegg, drift, gjenoppretting og øvrige tiltak som oppfyller kravene i denne forskriften.
§2.10	**Internkontrollsystem** KBO-enheter skal ha et internkontrollsystem som dokumenterer at det er etablert en systematikk for å sikre etterlevelse av kravene i energiloven kapittel 9, energilovforskriften § 3-5 bokstav c, § 5-3 bokstav c og bestemmelser gitt i eller i medhold av denne forskrift. Internkontrollsystemet skal inneholde dokumentasjon for at alle tiltak etter kravene i første ledd er på plass og fungerer etter sin hensikt. Internkontrollsystemet skal holdes oppdatert og gjennomgås slik at det gjenspeiler faktisk tilstand. Internkontrollsystemet skal være tilrettelagt for gjennomføring av tilsyn i samsvar med de krav som er stilt.
Kapittel 6	**Informasjonssikkerhet** I kraftberedskapsforskriften finnes en rekke krav til informasjonssikkerhet, og god veiledning finnes hos NVE.
Kapittel 7	**Beskyttelse av driftskontrollsystem** I kraftberedskapsforskriften finnes en rekke krav til beskyttelse av driftskontrollsystem, og god veiledning finnes hos NVE.

I tillegg til energiloven, sikkerhetsloven og kraftberedskapsforskriften, har norske myndigheter nå vedtatt en helt ny lov om digital sikkerhet, som skal bidra til å redusere sårbarheter i norske virksomheter.

BEHOV FOR ØKT SIKKERHET I NORSKE VIRKSOMHETER- NY LOV OM DIGITAL SIKKERHET

Den nye loven om digital sikkerhet[20] er et viktig bidrag for å redusere digitale sårbarheter både i samfunnet og i den enkelte virksomhet i Norge. Den nye sikkerhetsloven er bygget på EUs NIS-direktiv, og omfatter også skytjenester. Konsekvenser for omfattede samfunnskritiske norske virksomheter er at de får mer ansvar for å **beskytte seg mot cyberkriminalitet**, de forpliktes til å **overholde digitale sikkerhetskrav** og de må **varsle om alvorlige digitale hendelser**.

Dette vil ikke omfatte virksomheter som fra før er underlagt strengere sektorvise reguleringer, som for eksempel virksomheter som er omfattet av kraftberedskapsforskriften.
Virksomheter som er omfattet må gjennomføre jevnlige risikovurderinger for å identifisere potensielle trusler og sårbarheter i tjenestene som tilbys, og iverksette tiltak for å redusere risikoen. Et godt rammeverk for å gjøre et godt arbeid her, er Nasjonal sikkerhetsmyndighet (NSM) sine grunnprinsipper for IKT-sikkerhet.

Merk: Loven om digital sikkerhet har ikke trådt i kraft per april 2024.
Sentrale bestemmelser i ny lov om digital sikkerhet er: [21]

LOV OM DIGITAL SIKKERHET	
§1	**Formål:** Loven skal bidra til å sikre grunnleggende krav til digital sikkerhet i virksomheter med særlig betydning for samfunnet ved å forebygge, avdekke og motvirke uønskede hendelser i nettverks- og informasjonssystemer som brukes for å levere samfunnsviktige tjenester og digitale tjenester. Loven skal også legge til rette for sikkerhet i IKT-produkter, IKT-tjenester og IKT-prosesser.
§2	**Virkeområde** Utdrag: Loven gjelder for a. tilbydere av samfunnsviktige tjenester etter § 6 i sektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur b. tilbydere av digitale tjenester etter § 9.
§ 4	**Definisjoner** I denne loven menes med 1. nettverks- og informasjonssystemer: a. elektronisk kommunikasjonsnett som nevnt i ekomloven § 1-5 nr. 2 b. en enhet eller en gruppe av sammenkoblede eller beslektede enheter som behandler digitale data automatisk ved hjelp av et program c. digitale data som lagres, behandles, innhentes eller overføres ved hjelp av elementer som nevnt i bokstav a eller b for at dataene skal kunne driftes, vernes, beskyttes eller vedlikeholdes. 2. sikkerheten i nettverks- og informasjonssystemer: evnen nettverk eller informasjonssystemer har til å tåle, på et gitt tillitsnivå, enhver handling som går ut over tilgjengeligheten, autentisiteten, integriteten eller tilliten til lagrede, overførte eller behandlede data eller tilknyttede tjenester som tilbys eller er tilgjengelige via slike nettverks- og informasjonssystemer 3. hendelse: enhver hendelse med negativ virkning på sikkerheten i nettverks- og informasjonssystemer.

[20]Prop. 109 LS (2022–2023)
https://www.regjeringen.no/no/dokumenter/prop.-109-ls-20222023/id2975558/?ch=11

[21] Lovdata, Lov om digital sikkerhet: https://lovdata.no/dokument/LTI/lov/2023-12-20-108

§ 7	**Krav om sikkerhet for tilbydere av samfunnsviktige tjenester** En tilbyder av en samfunnsviktig tjeneste skal gjennomføre en **risikovurdering** av nettverks- og informasjonssystemer som benyttes for å levere tjenesten. Tilbyderen skal iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak som samlet skal sørge for et sikkerhetsnivå som er tilpasset risikoen. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det blant annet ses hen til den teknologiske utviklingen. Tilbyderen skal iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser, slik at tjenesteleveransen kan opprettholdes.
§ 8	**Krav om varsling for tilbydere av samfunnsviktige tjenester** En tilbyder av en samfunnsviktig tjeneste skal uten unødig opphold og uten hinder av taushetsplikt varsle det organet Kongen utpeker, om hendelser som virker betydelig inn på tjenesteleveransen. Ved vurderingen av om innvirkningen er betydelig, skal det blant annet legges vekt på antallet brukere som påvirkes, hendelsens varighet og størrelsen på det geografiske området som berøres.

OPPSUMMERING AV NASJONALE LOVER OG REGLER FOR ENERGI- OG KRAFTSEKTOREN

Kraft-og energisektoren er en samfunnskritisk bransje for Norge. Vår gjennomgang av lover og regler for kraftsektoren, viser da også en tilhørende sterkt regulert bransje som korresponderer med hvor samfunnskritisk sektoren er. Kraftforsyningen er samfunnskritisk infrastruktur, og egne reguleringer knyttet til beredskap og informasjonssikkerhet finnes **i energiloven**. Energiloven inneholder krav til produksjon, omforming, overføring, omsetning, fordeling og bruk av energi.

Sikkerhetsloven pålegger mange virksomheter i Norge et lederansvar for sikkerhet. Dette innebærer at de regelmessig skal vurdere risiko og gjennomføre øvelser, samt dokumentere arbeidet. I tillegg foreligger det en varslingsplikt, som gjør at sikkerhetsmyndighetene og andre myndigheter skal varsles dersom visse forhold inntreffer.

Forskrift for sikkerhet og beredskap i kraftforsyningen pålegger mange virksomheter i Norge et lederansvar for sikkerhet, at de regelmessig skal vurdere risiko, at de regelmessig skal gjennomføre øvelser, og at de skal dokumentere arbeidet. I tillegg foreligger det en varslingsplikt, som gjør at sikkerhetsmyndighet og andre myndigheter skal varsles dersom visse forhold inntreffer.

Lov om digital sikkerhet vil for omfattede samfunnskritiske norske virksomheter gi økt ansvar for å beskytte seg mot cyberkriminalitet, de forpliktes til å overholde digitale sikkerhetskrav og de må varsle om alvorlige digitale hendelser. Den nye loven om digital sikkerhet gjelder ***ikke*** virksomheter som fra før av er omfattet av kraftberedskapsforskriften. Konsekvensene for beslutningstakere i kraftsektoren vil allikevel være merkbare, ved at andre sektorer som ikke tidligere har hatt disse minstekravene, nå må heve sin motstandskraft. Dette må de gjøre innenfor eksisterende marked med de begrensningene som der finnes i forhold til tilgjengelige kompetente ressurser på sikekrhetsområdet. Dette vil medføre at **kraftsektoren nå får økt konkurranse om tilgjengelige sikkerhetsressurser og tjenester.**

Loven om digital sikkerhet har ikke trådt i kraft per juni 2024, og det kan komme forskrift som gjennomfører loven. Dette er per juni 2024 ikke avklart.

I tillegg til eksisterende og strenge nasjonale lover og regler for kraft- og energisektoren, vil nye omfattende reguleringer gjennom nye EU-direktiv gjøre at beslutningstakere i kraft- og energisektoren må **investere mer i sikkerhetstiltak og kompetanse** fremover. NIS2-direktivet, CER-direktivet, Cyber Resilience Act, Cybermotstandsdirektivet og Cybersikkerhetsforordningen

pålegger medlemsstater og omfattede virksomheter nye plikter og gir samtidig nye muligheter til å styrke motstandskraft og konkurransekraft. Se også oppsummeringen av europeiske lover og regler som påvirker Norge.

OPPSUMMERING LOVER OG FORSKRIFTER FOR ENERGISEKTOREN

Illustrasjonen nedenfor viser viktige lover og regler for energi- og kraftsektoren, som inkluderer både relevante EU-regelverk som blir EØS-relevante, og nasjonale regler. (Ikke- uttømmende liste).

Lover og regler om sikkerhet for energisektoren. Ikke-uttømmende liste. Kilde: Radar Norway, 2024.

Gjennomgangen av lover og forskrifter som gjelder for kraftbransjen, viser at Norge har et sterkt regelverk for sikkerhet og beredskap. Hvordan står det da til med den faktiske etterlevelsen av de strenge reglene? Har norsk kraftsektor tilstrekkelig motstandskraft? I det følgende gjennomgår vi nåsituasjonen for IKT-sikkerheten innen kraftforsyningen.

IKT-SIKKERHETEN INNEN KRAFTFORSYNINGEN- NÅSITUASJON

Faktisk etterlevelse må sikres gjennom godt risikobasert sikkerhetsarbeid i virksomhetene, og vi vil nå gjennomgå nåsituasjonen for IKT-sikkerheten kraftsektoren, før vi kommer med noen anbefalinger på hva beslutningstakere bør gjøre for å **styrke sin motstandskraft**.

Flere rapporter avdekker at **IKT-sikkerheten må styrkes i kraftbransjen**. Riksrevisjonens rapport om IKT- sikkerheten i kraftforsyningen, KraftCerts rapporter om uønskede hendelser, samt NVEs rapporter om avvik innen IKT-sikkerhet, bekrefter at beslutningstakere innen kraftsektoren må arbeide mer systematisk med IKT-sikkerhet i sine virksomheter. I det følgende gjennomgår vi hvilke områder som peker seg ut på IKT-sikkerhetsområdet i kraftsektoren, før vi til slutt gir noen anbefalinger til hvordan beslutningstakerne kan jobbe systematisk med IKT-sikkerhet og sikkerhet i virksomhetene.

RIKSREVISJONENS RAPPORT OM IKT-SIKKERHET I KRAFTFORSYNINGEN

Riksrevisjonen påpeker i sin tilsynsrapport av 2021 følgende om IKT-sikkerheten innen kraftforsyningen: Bruk av ny teknologi, skyløsninger og utenlandske leverandører og integrering av ulike systemer som er koblet til internett øker risikoen for IKT-hendelser i kraftforsyningen.

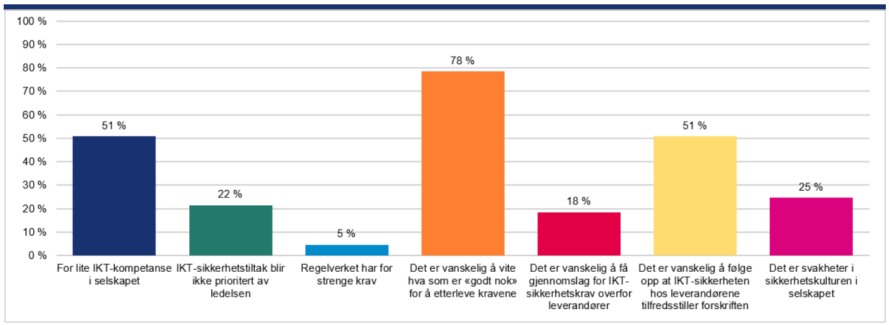
I Norge er det om lag 170 KBO-enheter i kraftforsyningen, og Riksrevisjonen påpeker at NVE de siste seks årene har gjennomført om lag fem IKT-sikkerhetstilsyn hvert år. I perioden 2017–2019 førte NVE IKT-sikkerhetstilsyn med om lag halvparten av selskapene som har de viktigste driftskontrollsystemene, det vil si systemene som brukes til å styre og overvåke strømforsyningen.[22]

Kravene til IKT-sikkerhet i kraftforsyningen i norsk regelverk er strenge sammenlignet med tilsvarende krav i andre europeiske land og andre sektorer i Norge, påpeker Riksrevisjonen. Strengt regelverk er derimot ingen garanti for faktisk etterlevelse, noe nedenstående gjennomgang viser.

UTFORDRINGER MED Å ETTERLEVE KRAV I REGELVERKET

Riksrevisjonens rapport avdekker også at nærmere 80 prosent av IKT-sikkerhetskoordinatorene oppga «Det er vanskelig å vite hva som er 'godt nok' for å etterleve kravene» som en årsak til hvorfor det er utfordrende å etterleve enkelte av kravene i regelverket. Over halvparten svarer også at det er vanskelig å følge opp at IKT-sikkerheten hos leverandørene tilfredsstiller forskriften.

Figur 3 IKT-sikkerhetskoordinatorenes svar på hvorfor det er utfordrende å etterleve enkelte av kravene i regelverket (N = 65)



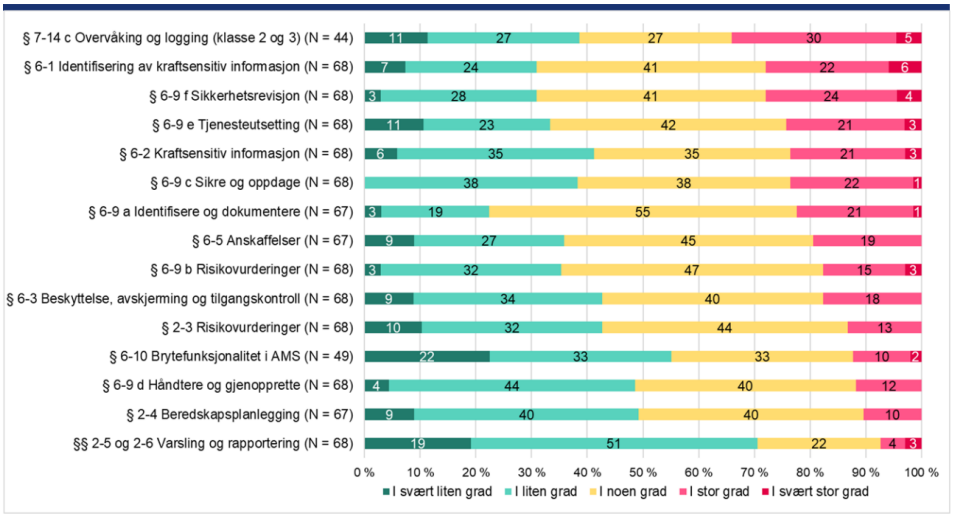
Kilde: Riksrevisjonen, Dokument 3:7 (2020–2021): https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/nves-arbeid-med-ikt-sikkerhet-i-kraftforsyningen.pdf

HVILKE KRAV ER MEST UTFORDRENDE Å ETTERLEVE?

Kravene som høyest andel koordinatorer oppga som utfordrende å etterleve, er kravene til overvåking og logging i driftskontrollsystemer, identifisering av kraftsensitiv informasjon samt sikkerhetsrevisjon og tjenesteutsetting.

[22] Riksrevisjonen, Dokument 3:7 (2020–2021): https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/nves-arbeid-med-ikt-sikkerhet-i-kraftforsyningen.pdf

Figur 2 IKT-sikkerhetskoordinatorenes svar på om utvalgte krav er utfordrende å etterleve



Kilde: Riksrevisjonen, Dokument 3:7 (2020–2021): https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/nves-arbeid-med-ikt-sikkerhet-i-kraftforsyningen.pdf

OVERVÅKING OG LOGGING I DRIFTSKONTROLLSYSTEMER

For å kunne iverksette tiltak for å redusere sårbarheter, forutsetter det god oversikt, gjennom overvåking og logging. I kraftberedskapsforskriften stilles det krav om at virksomheten må ha informasjon om egne sikkerhetsbrudd, herunder logger, og disse må registreres og lagres trygt, beskyttet og med minimal risiko for uautorisert endring. NVE anbefaler derfor at virksomhetene har tilgang til et sikkerhetsoperasjonssenter (SOC). KraftCERT kan gi råd i forbindelse med anskaffelse av slik tjeneste. [23]

SIKKERHETSREVISJON

Riksrevisjonens undersøkelse viste at sikkerhetsrevisjoner var utfordrende å etterleve for flere av respondentene. NVE skriver i sin veiledning til kraftberedskapsforskriften at revisjon av iverksatte sikringstiltak for digitale informasjonssystemer skal være en gjentakende aktivitet. Organisering av sikkerhetsarbeidet, inkludert plassering av ansvar, og tiltak for å beskytte kraftsensitiv informasjon mot uautorisert tilgang hører hjemme her. Resultatene og konklusjonene fra sikkerhetsrevisjonene må også dokumenteres.

TJENESTEUTSETTING

Tjenesteutsetting kompliseres av at det er komplekse leverandørkjeder. Sårbarheten i sammenkoblede IT-systemer avhenger av det svakeste leddet, og helhetlig tilnærming og inkludere alle deler av systemet er viktig når aktører vurderer risiko i verdikjeder og leverandørkjeder (NVE, 2017). NSM og PST hevder i sine trusselvurderinger at norske virksomheter også er utsatt for risiko for cyberangrep på kritiske samfunnsfunksjoner. [24]

Leverandørkjedenes kompleksitet kan gjøre det utfordrende å ha full oversikt over alle ledd, men oversikt er viktig for å vurdere hvor sikkerhetstiltak må implementeres. Et godt arbeid med leverandørkjedesikkerhet forutsetter at virksomhetene får **oversikt over sårbarhetene i**

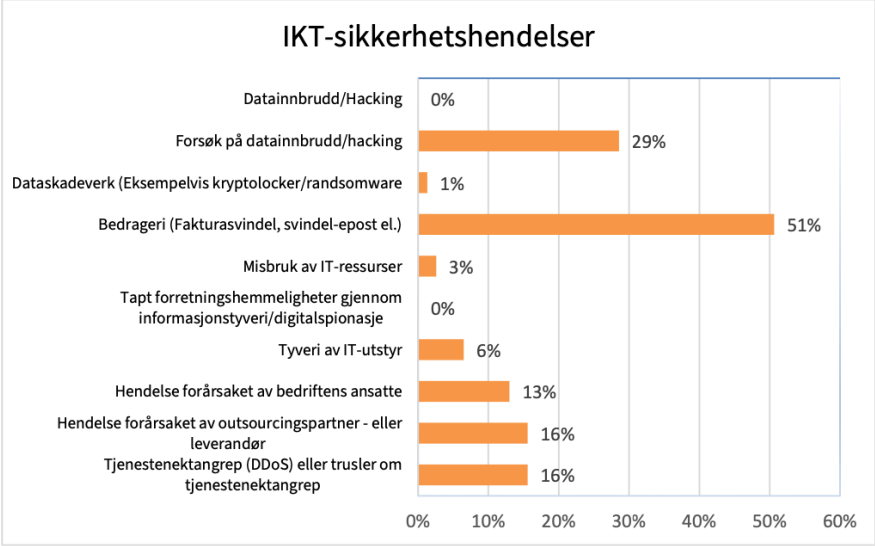
[23] NVE, Veiledning til kraftberedskapsforskriften: https://veiledere.nve.no/kraftberedskapsforskriften/kapittel-7-beskyttelse-av-driftskontrollsystem/7-7-handtering-av-feil-sarbarheter-og-sikkerhetsbrudd/

[24] NSM, Risiko 2023: https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

leverandørkjedene. I tillegg avdekket Riksrevisjonens casestudie at det var flere mangler i selskapenes arbeid med å risikovurdere IKT-systemer som behandler kraftsensitiv informasjon, og i gjennomføringen av evalueringer.

HENDELSESSTATISTIKK FRA KRAFTCERT

Hendelsesstatistikk fra KraftCERT viser et fortsatt økende antall IKT- sikkerhetsrelaterte hendelser i kraftsektoren, der ***bedrageri, tjenestenektangrep*** og ***forsøk på datainnbrudd*** er de vanligste hendelsestypene.



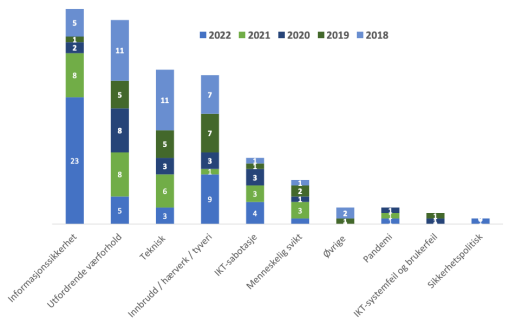
Kraftberedskapsforskriften krever at virksomhetene varsler NVE ved alle ekstraordinære hendelser. Uønskede hendelser i digitale informasjonssystemer skal varsles til den beredskapsmyndigheten bestemmer, herunder KraftCERT, og skal også rapporteres i etterkant av håndteringen.

Kilde: NVE, 2023. Andel virksomheter der en IKT-sikkerhetshendelse har hatt konsekvens for virksomhetsdrift eller funksjonen til driftskontrollsystemer mellom februar 2022 – mai 2023. Svaret oppgis i prosent. N = 74

KraftCERT rapporterer at det fra 2019 til 2021 har vært en økende trend for håndterte hendelser vært økende. Det totale antall saker hos KraftCERT økte med 13,3 % fra 4979 i 2021 til 5645 i 2022.[25]

I rapporten fremkommer det også at KraftCERT ikke kjenner til at **driftskontrollsystem** i Norge har blitt rammet av IKT-hendelser de siste årene. Utviklingen i antall komponenter i driftskontrollsystemene, sammen med økt automatisering og digitalisering, gjør allikevel at kraftbransjen **må anse driftskontrollsystemene som et mulig angrepsmål**.

RISIKO- OG VESENTLIGHETSVURDERINGER FRA NORGES VASSDRAGS- OG ENERGIDIREKTORAT (NVE)



Figur 1: Uønskede hendelser 2018-2022

NVEs risiko- og vesentlighetsvurderinger for årene 2017–2020, skriver NVE at digitaliseringen har ført til **kompetanseutfordringer**, og at både NVE og bransjen er avhengige av å styrke kompetansen på IKT-sikkerhetsområdet.

NVEs studie av IKT-sikkerhetstilstanden i 2017 (NVE-Rapport 2017:90), viste at 8 av 10 virksomheter i kraftbransjen er

[25] NVE, 2023-27: https://publikasjoner.nve.no/rapport/2023/rapport2023_27.pdf

avhengige av leverandørene for å håndtere hendelser i sine IT- og driftskontrollsystemer og gjenopprette systemene dersom de feiler. [26] NVE oppsummerer en undersøkelse fra 2023 kraftforsyningens beredskap mot cyberangrep. Rapporten peker på viktigheten av å ha **beredskapsplaner** og ikke minst **øvelser** som bidrar til å realitetsorientere og validere og utvikle planene.[27]

I rapporten fra NVE har majoriteten av virksomhetene som har svart på undersøkelsen en beredskapsplan og har etablert beredskapsstrukturer. Når det gjelder rutiner for øvelser og evaluering etter øvelser og hendelser er disse tiltakene i mindre utstrekning på plass.

Kraftberedskapsforskriften §§ 1-5 og 2-4 lovfester at virksomheter skal ha en **oppdatert beredskapsplan som bygger på risikovurderinger**. Beredskapsplanen skal bidra til å «forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner (…)» (kraftberedskapsforskriften § 1-5). NVE stiller krav til KBO-enheter om å sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas (§ 6-9). Det er en direkte og tett kobling mellom risikovurderinger og digital beredskap, skriver NVE i rapporten om IKT-sikkerheten i kraftforsyningen 2023. [28]

Leverandørkjedenes kompleksitet kan gjøre det utfordrende å ha full oversikt over alle ledd, men oversikt er viktig for å vurdere hvor sikkerhetstiltak må implementeres. Et godt arbeid med leverandørkjedesikkerhet forutsetter at virksomhetene får oversikt over sårbarhetene i leverandørkjedene.

UØNSKEDE HENDELSER I KRAFTSEKTOREN 2018-2022

NVE har utarbeidet en oversikt over uønskede hendelser i kraftsektoren for årene 2018-2022, og året 2022 skiller seg ut ved at NVE mottok klart flest rapporter innen kategorien **informasjonssikkerhet**. I denne kategorien er hendelser hvor kraftsensitiv informasjon har kommet på avveie inkludert. I tillegg er uvanlig interesse for kraftforsyningsanlegg (fotografering fra bakken eller fra droner) basert på observasjoner fra KBO inkludert i oversikten. I følge KraftCERT var beredskapen forhøyet i alle sektorer i 2022, og det ble sendt ut flere varsler i 2022 enn tidligere og antall sårbarheter med høy kritikalitet økte.

DE TI VANLIGSTE AVVIKENE VED TILSYN MED KRAFTBEREDSKAP OG VEDLIKEHOLD

NVE har i perioden 2015-2018 gjennomført 196 tilsyn og funnet i alt 641 avvik. Figuren under viser de ti vanligste avvikene, noe som utgjør 77 % av alle avvikene.

[26] NVE: IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen. Rapport nr. 1, 2020: https://publikasjoner.nve.no/rapport/2020/rapport2020_01.pdf

[27] NVE, rapport nr 27/2023, IKT-sikkerheten i kraftforsyningen 2023: https://publikasjoner.nve.no/rapport/2023/rapport2023_27.pdf

[28] NVE, rapport nr 27/2023, IKT-sikkerheten i kraftforsyningen 2023: https://publikasjoner.nve.no/rapport/2023/rapport2023_27.pdf

Kilde: NVE, Tilstandsvurdering av forsyningssikkerhet og beredskap i kraftforsyningen, 2019.[29]

Avvikene viser hva tilsynet har funnet i sine revisjoner, og omfatter ikke den generelle sikkerhetstilstanden i bransjen. Avvikene viser allikevel hvilke områder som har vært mangelfulle i de deler av bransjen der tilsynet har vært utført. Mangler har i stor grad vært funnet i risikovurderinger, i forhold til beredskapsplaner, samt fysisk krav til sikring og tilgang på materiell. Avvikslisten viser også flere avvik knyttet til evaluering av hendelser og øvelser.

OPPSUMMERING AV NÅSITUASJONEN FOR IKT-SIKKERHETEN I KRAFTSEKTOREN

Kraftsektoren har flere utfordringer knyttet til IKT-sikkerhet og motstandskraft mot hendelser, samt evne til å håndtere hendelser. Mange virksomheter opplever utfordringer med risikostyring, tjenesteutsetting og overvåking og logging. Flere uttrykker utfordringer med identifisering av kraftsensitiv informasjon, gjennomføring av sikkerhetsrevisjoner og evaluering og testing. Vår analyse viser at det er behov for **økt motstandskraft og økt modenhet i risikostyring i kraftsektoren.**

Nåsituasjon for IKT-sikkerheten i kraftsektoren. Kilde: Radar Norway, 2024.

ANBEFALINGER TIL BESLUTNINGSTAKERE I KRAFTSEKTOREN

Gjennomgangen ovenfor av nåsituasjonen for IT-sikkerhet i kraft- og energibransjen, samt relevant regelverk på området, viser områder beslutningstakere bør prioritere for å **styrke motstandskraften og konkurransekraften** fremover. Dette er anbefalinger til beslutningstakere der analyse av nåsituasjonen i virksomheten er essensielt for at tiltakene skal være tilpasset virksomhetens behov. Vi kommer også med generelle anbefalinger til alle beslutningstakere uavhengig av sektor helt til slutt i rapporten. Dette fordi den generelle økningen av reguleringer vil gi ringvirkninger på tvers av sektorer.

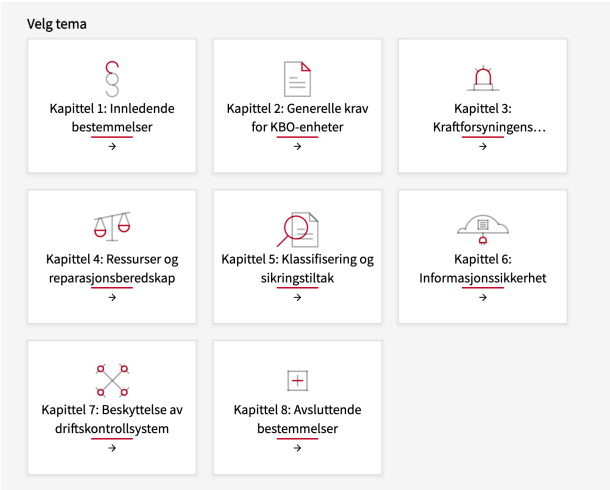
[29] NVE, Fakta 10/2019: https://publikasjoner.nve.no/faktaark/2019/faktaark2019_10.pdf

1. **Integrer sikkerhet i virksomhetens aktiviteter og etablér styringssystem for informasjonssikkerhet**

Virksomhetene bør integrere sikkerhet i virksomhetens aktiviteter og å etablere et styringssystem for informasjonssikkerhet som ivaretar systematikken for aktivitetene i IKT-sikkerhetsarbeidet. Dette kan illustreres slik:

Illustrasjon av styringen av IKT-sikkerhetsarbeidet. Kilde: Riksrevisjonen, NSM og NVE.

Veiledninger til god sikkerhetsstyring finnes på NSMs sider. Alle virksomheter må etablere en helhetlig risikostyringsprosess. I bunn og grunn handler det om å spørre seg: Hva er de kritiske områdene vi bør adressere, og hvor skal vi starte? Hvordan kan vi sikre, vedlikeholde, overvåke og forbedre IKT-systemene våre?



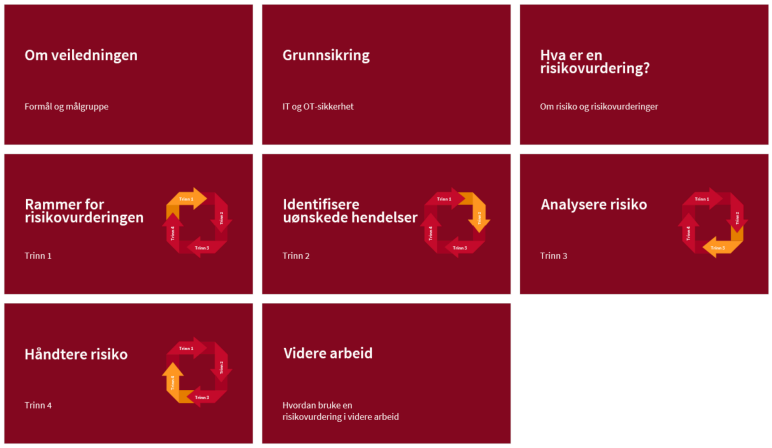
NVE 2024, Veiledning til kraftberedskapsforskriften.

2. **Les sikkerhetsloven, energiloven samt kraftberedskapsforskriften. Bruk veilederne.**

NSM har flere veiledere og håndbøker til sikkerhetsloven[30], og NVE har i 2024 utgitt en oppdatert veileder til kraftberedskapsforskriften, som bør leses grundig av ledergruppene og beredskapsansvarlige i kraftsektoren. Veilederen er delt inn i kapitler som speiler forskriftens oppbygging. Veilederen gir gode råd for hvert enkelt krav i forskriften, og vil være et godt verktøy for å øke motstandskraft og redusere risiko.

[30] NSM, Veiledere til sikkerhetsloven: https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/

3. Les veileder for risikovurderinger og informasjonssikkerhet i IT- og OT-systemer



Gjennomgang av veilederen bør kompletteres av en gjennomgang av veileder for risikovurderinger generelt og informasjonssikkerhet og digital sikkerhet i IT- og OT-systemer spesielt, som også er utarbeidet i 2024 av NVE. Den er spesielt rettet mot små -og mellomstore bedrifter, men gir også gode råd til de større virksomhetene.

Kilde: NVE veiledning, 2024: Veiledning for risikovurdering av IT og OT, skrevet av KPMG[31].

Økt integrasjon mellom IT og OT gjør infrastrukturen mer kompleks, det blir vanskeligere å holde oversikt og trusselbildet endrer seg. Behovet for kontroll og oversikt øker, og man kan ikke håndtere IT og OT som to separerte domener. Veiledningen gir en trinnmodell for gjennomføring av risikovurderinger, og gir eksempler på hvordan kraftselskaper kan arbeide med å øke sin motstandskraft.

4. Bruk sjekklisten for IKT-sikkerhet i anskaffelser og tjenesteutsetting

Virksomheter som skal anskaffe IKT-tjenester i energisektoren, bør benytte sjekklisten som er utarbeidet av NVE: Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting. Sjekklisten bygger på Energiloven og kraftberedskapsforskriften, samt veiledere fra Nasjonal sikkerhetsmyndighet (NSM), rapporter fra Norges vassdrags- og energidirektorat (NVE) og beste praksis. NVE har også utarbeidet en rapport om hvordan sette krav til IKT-sikkerhet i anbud og kontrakter, som anbefaler må- og bør-krav rettet spesielt mot små og mellomstore nettselskap i kraftforsyningen til bruk i anbud- og anskaffelsesprosesser. Anbefalingene gjelder krav ved anskaffelse av både IT og OT, og ser spesielt på leverandørkjedene.[32]

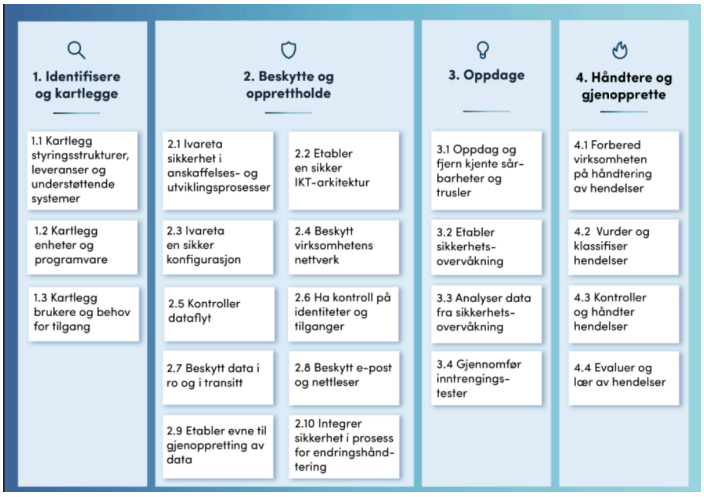
5. Bruk NSMs grunnprinsipper for IKT-sikkerhet

Enhver virksomhet har både felles og unike risikoer, og har varierende risikovillighet og toleranse, spesifikke mål og tiltak for å oppnå disse målene. Grunnprinsippene er en måte å operasjonalisere arbeidet med økt motstandskraft på.

---

[31] NVE veiledning, 2024: Veiledning for risikovurdering av IT og OT, skrevet av KPMG: https://publikasjoner.nve.no/veileder/2024/veileder2024_02.pdf

[32] NVE Ekstern rapport 5/2023: Sett krav til IKT-sikkerhet i anbud og kontrakter – en forstudie: https://publikasjoner.nve.no/eksternrapport/2023/eksternrapport2023_05.pdf



Grunnprinsipper for IKT-sikkerhet. Kilde: NSM.

Grunnprinsippene for IKT-sikkerhet gir råd for å beskytte informasjonssystemer, data og tjenester mot uautorisert tilgang, skade eller misbruk. Støtteverktøy hos NSM er blant annet digital veiledning, samt tilhørende Excel-fil for gjennomføring og prioritering av tiltak. [33]

6. Hold deg informert om kommende lover

Gjennomgangen av regelverkene over ligger i første del av rapporten, og er sammenfattet i Bilag A, regulatorisk rammeverk. Forbered egen ledergruppe på hvilke **virksomhetsstyringsaktiviteter** som må planlegges. Kommende regler på cybersikkerhet, kritiske enheters motstandsdyktighet, samt cybersikkerhetsforordning og CER-direktivet peker seg ut. Bruk våre anbefalinger til å analysere din virksomhets nåsituasjon opp mot ønsket situasjon, og finn de nødvendige tiltak som skal til for å styrke motstandskraft i egen virksomhet.

OPPSUMMERING: ANBEFALINGER TIL BESLUTNINGSTAKERE I KRAFTSEKTOREN

Beslutningstakere i kraftsektoren bør gjøre flere grep for å **styrke motstandskraften og konkurransekraften** fremover. Oppsummert kan våre anbefalinger visualiseres slik:

Illustrasjon av forbedringsområder innen sikkerhet innen kraftsektoren. Kilde: Radar Norway. 2024.

[33] NSMs støtteverktøy for grunnprinsippene for IKT-sikkerhet: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/stotteprodukter/#:~:text=St%C3%B8tteverkt%C3%B8y%20for%20NSMs%20grunnprinsipper%20for%20IKT%2Dsikkerhet%202.0%C2%A0%20(XLSX%2C%20128KB)

Kraft- og energisektoren er en samfunnskritisk sektor, og det er flere grep som kan styrke motstandskraften i virksomhetene. Kraft- og energisektoren har kommet lengre enn mange andre sektorer hva gjelder modenhet. Neste dypdykk er derfor mat- og prosesseringsindustrien, som i motsetning til kraftsektoren ikke tidligere har hatt et strengt regelverk på IKT-sikkerhet, men som nå blir omfattet av nye regler som CER-direktivet og NIS2-direktivet.

Mat-og prosesseringsindustrien har visse likheter med kraftsektoren grunnet høy andel IT/OT-utbredelse for produksjonsprosesser, men har visse ulikheter siden sektoren ikke har hatt sektorspesifikke regler for IT-sikkerhet som er like omfattende som kraftsektoren. Matsektoren må nå være forberedt på strengere regler på IT-sikkerhet fremover. Vi går gjennom bransjens IKT-sikkerhet, eksisterende regler, og nye regler som påvirker beslutningstakere innen mat- og prosesseringsindustrien.

BRANSJEPERSPEKTIV PÅ MOTSTANDSKRAFT: MAT- OG PROSESSERINGSINDUSTRIEN

Vi skal nå ta for oss en av de omfattede sektorene i det nye CER-direktivet, nærmere bestemt mat- og prosesseringsindustrien. Vi gir først en analyse av nåsituasjonen for utviklingen, modenheten og IKT-sikkerheten i bransjen, før vi gjennomgår nasjonale lover og regler som påvirker beslutningstakerne i sektoren. Til slutt i bransjegjennomgangen gir vi noen anbefalinger på hva beslutningstakere i bransjen nå bør gjøre for å styrke sin motstandskraft og sikkerhet.

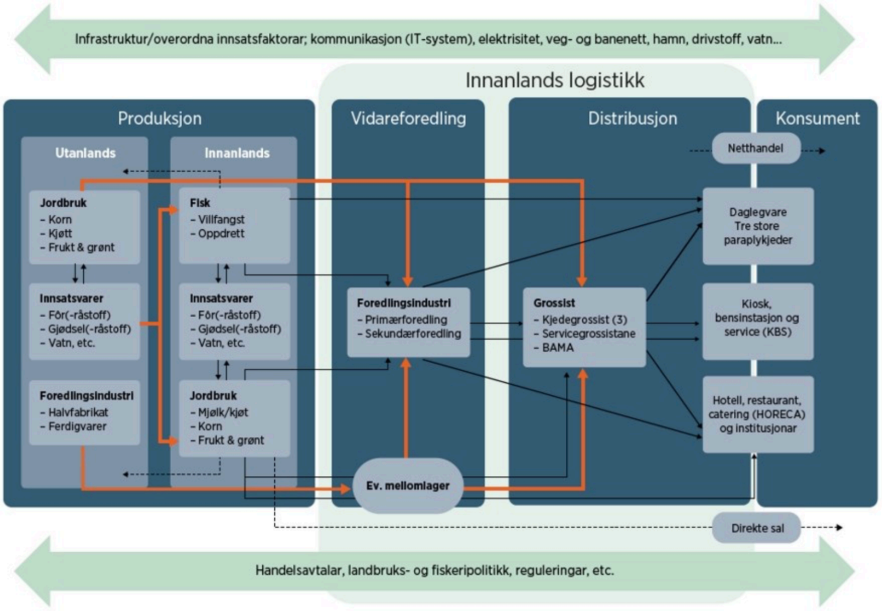
DIGITAL MODENHET I MAT- OG PROSESSERINGSINDUSTRIEN

Norge har et høyteknologisk og transportintensivt matproduksjons- og distribusjonssystem. Dette forutsetter at vesentlige innsatsfaktorer fungerer som de skal, herunder energi, arbeidskraft, fôr, vann og kapital. Økt digitalisering og avhengighet av teknologi i alle faser av produksjon, distribusjon og salg av mat, gjør at cyberangrep kan forstyrre og skade hele matforsyningsprosessen. Risikoen omfatter alt fra små gårder, fabrikker, lagringsanlegg og distribusjonssentre.

Gjennomgangen av risikofaktorer, både geopolitisk, økonomisk og på trusselbildet, viser at angrep rettet mot matforsyningskjeden kan ha alvorlige konsekvenser. CER-direktivet og det nye NIS2-direktivet fra EU omfatter derfor også matforsyning.

Norsk matforsyningsbransje er fra før av omfattet av regelverk knyttet til matsikkerhet, herunder krav til hygiene i animaliehygieneforskriften og næringsmiddelhygieneforskriften. Det kommende loven om digital sikkerhet forventes å tre i kraft snart, men den omfatter ikke mat- og prosesseringsindustrien direkte. Den omfatter dog tilstøtende sektorer, som forsyner mat- og prosesseringsindustrien med innsatsfaktorer, som kommunikasjon, (IT-systemer) elektrisitet, energi, transport med mer. Det er også ventet at arbeidet med NIS2 i Norge vil skje i løpet av 2024, og mat- og prosesseringsindustrien må forvente å bli omfattet av NIS2-rammeverket. CER-direktivet omfatter spesifikt matprosesseringsindustrien, og arbeidet forventes også å skje snart i norsk sammenheng.

En risiko- og sårbarhetsanalyse utført av Direktoratet for samfunnssikkerhet og beredskap (DSB) i 2017 viser hvor kompleks også verdikjeden for matproduksjon- og forsyning er i Norge. Illustrasjonen er hentet fra DSB.



Verdikjeden for matproduksjon- og forsyning i Norge, inkludert kritiske innsatsfaktorer og politiske rammevilkår. Kilde: Direktoratet for sikkerhet og beredskap, Risiko- og sårbarhetsanalyse av norsk matforsyning, 2017.

Mat- og drikkenæringen er den største fastlandsindustrien i Norge. Produksjon av mat og drikke er også en av få komplette verdikjeder i Norge, og består av mange ulike bransjer.[34] Mat- og drikkenæringen er en energikrevende næring, hvor elektrisitet er svært dominerende i de fleste av bransjene. Energikostnadene i mat- og drikkenæringen er dermed svært eksponert for svingninger i strømprisen. Høye energikostnader og økte importkostnader ble forsterket av en svak norsk kronekurs, og samlet sett har bedriftene blitt rammet av svært mange kostnadsøkninger over en lengre tidsperiode. Dette påvirker både lønnsomhet og konkurranseevne i matindustrien. Vår gjennomgang av nye reguleringer, som for eksempel NIS2, vil medføre ytterligere økte kostnader og behov for økte investeringer i sektoren.

LOVER OG FORSKRIFTER OM SIKKERHET FOR MAT- OG PROSESSERINGSINDUSTRIEN

I Norge er ikke IKT-sikkerhet i matvareproduksjon regulert av en egen lov, men både Lov om næringsberedskap[35] og Matloven er relevante lover for sektorens generelle matberedskap[36]. Den kommende loven om digital sikkerhet omfatter ikke hele mat- og prosesseringsindustrien, og gjelder kun drikkevannsforsyningsvirksomheter på matsektoren. CER-direktivet vil også gjelde for kritiske entiteter innen matsektoren, og arbeidet med forberedelser bør være parallelle med arbeidet med NIS2-direktivet. Dette vil bli viktig som ledd i økt motstandskraft og konkurransekraft i matsektoren. Det kommende NIS2-regelverket derimot, fremhever matindustrien som en viktig sektor, og minimumsreglene i direktivet vil gjelde.

[34] NHO Mat og Drikke Konjunkturrapport 2023: nho-mat-og-drikke-konjukturrapport-2023v4.pdf (nhomd.no)

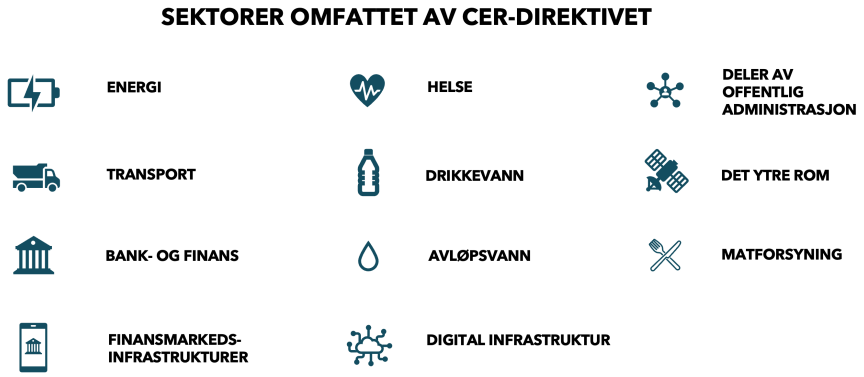
[35] Lov om næringsberedskap, https://lovdata.no/dokument/NL/lov/2011-12-16-65

[36] Matloven: https://lovdata.no/dokument/NL/lov/2003-12-19-124?q=matloven

EUROPEISKE LOVER SOM PÅVIRKER MAT- OG PROSESSERINGSINDUSTRIEN

CER-DIREKTIVET

CER-direktivet omfatter 11 bransjer, herunder mat- og prosesseringsindustrien, slik figur under viser.



CER-direktivets 11 sektorer. Kilde: Radar Norway

Det arbeides nå med hvordan reglene kan innføres i europeiske land. Sverige kommer med sin delutredning om CER-direktivet i september 2024, mens norske myndigheter fortsatt arbeider med sine vurderinger.

Medlemslandene må identifisere og lage en oversikt over kritiske enheter under de 11 sektorene og informere de kritiske enhetene om at de er identifisert og hvilke plikter dette gir. Identifikasjonen skal baseres på de nevnte risikovurderinger og en rekke kriterier, herunder om en hendelse vil ha betydelige forstyrrende virkning for leveringen av en tjeneste.[37] Flere norske matprosesseringsaktører må forberede seg på å bli utpekt som kritisk entitet, og må gjøre passende tiltak for å styrke sin motstandskraft.
Operatører som blir omfattet av CER-direktivet skal gjennomføre følgende tiltak:

- Gjennomføre regelmessige risikovurderinger som kan integreres i andre risikovurderingsprosesser, inkludert nasjonale nivåer;
- Opprettholde en operatørresiliensplan eller tilsvarende, inkludert bestemmelser om risikoredusering og beredskap, hendelseshåndtering og gjenoppretting. Planen bør beskrive ordninger angående:
    - Generelle beredskapstiltak;
    - Fysisk sikkerhet, med hensyn til både tradisjonelle og nye trusler;
    - Personellsikkerhetsstyring; og
    - Kontinuitetsplaner for virksomheten.
- Utnevne en enkelt kontaktperson for beskyttelses-/resilience-saker, som kobler operatøren sammen med andre interessenter, inkludert nasjonale kompetente myndigheter og andre kritiske infrastruktur-operatører;
- Delta i kapasitetsbyggende aktiviteter, inkludert opplæring og bevissthetshøyning for personalet; og
- Rapportere hendelser.

[37] Europalov, Direktiv om kritiske enheters motstandsdyktighet: https://europalov.no/rettsakt/direktiv-om-kritiske-enheters-motstandsdyktighet/id-28658

NIS2-DIREKTIVET OG PÅVIRKNING PÅ MAT- OG PROSESSERINGSINDUSTRIEN

Vi omtalte i den generelle regulatoriske analysen hvilke sektorer som er omfattet av NIS2- direktivet, og produksjon, videreforedling og distribusjon av mat omtales som en av de viktige sektorene som omfattes av kravene i direktivet.

Uavhengig av størrelsen på virksomhet, vil den gjelde din type virksomhet innen matsektoren, dersom din virksomhet dekkes av teksten henvist til i bilag 2:

SEKTOR:	TYPE AV VIRKSOMHET
PRODUKSJON, VIDEREFOREDLING OG DISTRIBUSJON AV MAT	Matbedrifter, som definert i artikkel 3, punkt (2), i forordning (EF) nr. 178/2002 fra Europaparlamentet og Rådet, som driver engrosdistribusjon og industriell produksjon og bearbeiding. Fra direktivet 178/2002 defineres «matvirksomhet» slik: Matvirksomhet" betyr enhver virksomhet, enten det er for profitt eller ikke, og enten det er offentlig eller privat, som utfører noen av aktivitetene knyttet til noen av stadiene i produksjon, bearbeiding og distribusjon av mat.

Dette betyr at alle produsenter og distributører av mat, over minimumsstørrelsen definert i direktivet, må forberede seg på innføringen av minstekravene i NIS2, og må iverksette tiltak i egen virksomhet. Dette berører nær 5,303 mellomstore og store bedrifter i EU. [38]

Minimumstiltakene er tidligere omtalt i kapittel om kraftsektoren og gjør at omfattede tilbydere må iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske tiltak for å håndtere **risiko i nettverk og informasjonssystemer.** Det kreves en risikostyringsmetode med en minimumsliste over grunnleggende sikkerhetselementer som må legges til grunn for sikkerhetsarbeidet, blant annet krav om at tilbydere håndterer cybersikkerhetsrisiko i **forsyningskjeder** og hos **leverandører**, planer for vedlikehold, overvåkning og testing samt bruk av krypto.

EUs egen gjennomgang av konsekvensene av innføringen av NIS2, beskriver utgiftskonsekvensene slik:[39]

For bedriftene som ville falle inn under omfanget av NIS-rammeverket, anslås det at virksomhetene vil få økning på maksimalt 22% av deres nåværende utgifter til IKT-sikkerhet for de første årene etter innføringen av det nye NIS-rammeverket (dette ville være 12% for selskaper som allerede er under omfanget av gjeldende NIS-direktiv). Imidlertid ville denne gjennomsnittlige økningen av utgifter til IKT-sikkerhet føre til en proporsjonal fordel, særlig på grunn av en betydelig reduksjon i kostnadene ved cybersikkerhetshendelser (anslått til 11,3 milliarder EURO over ti år).

Både NIS2-direktivet og CER-direktivet er ment å forbedre cybersikkerhet og motstandskraft over hele EU, gjennom å adressere både digitale (NIS2) og fysiske (CER) trusler.

Innkjøpere og beslutningstakere i matprosesseringsindustrien bør også ta hensyn til Cyber Security Act, om overgripende cybersikkerhetskrav for produkter med digitale elementer. Dette kan også føre til behov for utskifting av eldre infrastrukturer, som kan være både mindre sikre, men også mindre energieffektive og miljøvennlige. Nye krav vil innebære at produkter som dekkes av rettsakten må være konstruert slik at de ivaretar kravene til cybersikkerhet.

[38] EU EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT REPORT, NIS2 directive: https://ec.europa.eu/newsroom/dae/redirection/document/72174

[39] EU EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT REPORT, NIS2 directive: https://ec.europa.eu/newsroom/dae/redirection/document/72174

OPPSUMMERING LOVER OG FORSKRIFTER I MAT- OG PROSESSERINGSINDUSTRIEN

Matsektoren må forholde seg til økte krav til ledelsesinvolvering, og økte investeringer i sikkerhet, samt økte krav til leverandørstyring og hendelsesrapportering. For bedriftene som ville falle inn under omfanget av NIS-rammeverket, anslås det at virksomhetene vil få økning på maksimalt 22% av deres nåværende utgifter til IKT-sikkerhet for de første årene etter innføringen av det nye NIS-rammeverket. Følgende relevante europeiske og norske lover og regler for beslutningstakere innen IT for mat- og prosesseringsindustrien (ikke-uttømmende liste):

Kilde: Radar Norway, 2024.

IKT SOM VIKTIG DEL AV MAT- OG PROSESSERINGSINDUSTRIEN

Verdien av digital infrastruktur øker. Økt digitalisering i energiforsyningen og tettere sammenkobling av systemer og nettverk har gjort at de totale systemene blir mer komplekse, og det kan være utfordrende å sikre seg full oversikt. Dette øker risikoen for teknisk feil, menneskelig svikt og også for uautorisert inntrenging i systemene. Det utgjør en digital sårbarhet, som kan utnyttes.

Kunstig intelligens, stordataanalyse, bruken av sensorer og tingenes internett er med på å drive denne utviklingen videre. Bruk av nettverk- og informasjonssystemer er i kjernen av den videre digitale transformasjonen av matindustrien, slik den også er det i andre sektorer.

Digitale teknologier har transformert matproduksjon og produksjonsindustrier til dataprodusenter. Dette gjør at effektive datagovernance- og cybersikkerhetsstrategier må være på plass. EU går foran, og har vedtatt minimumstiltak for å styrke motstandsevnen til europeiske virksomheter, og nedenfor redegjør vi for hvordan den norske matsektoren blir omfattet av de kommende NIS2-reglene og CER-reglene samt hvordan den norske matsektoren bør arbeide for å sikre innføringen av minimumstiltakene innen cybersikkerhet.
Ekom-tjenester og IKT brukes for eksempel i produksjon, lagerstyring, distribusjon, ordre og informasjonsutveksling. [40] Forretningssystemer (ERP) er essensielle i distribusjonssystemene i mat- og prosesseringsindustrien. Dette er støttesystemer for prosessene rundt virksomhetene, som økonomi, lønn, HR, produksjon, innkjøp og salg.

[40] DSB, 2017, Risiko-og sårbarhetsanalyse av norsk matforsyning: Risiko- og sårbarhetsanalyse av norsk matforsyning–side 40 (dsbinfo.no)

IKT-SIKKERHETEN INNEN MAT- OG PROSESSERINGSINDUSTRIEN- NÅSITUASJON

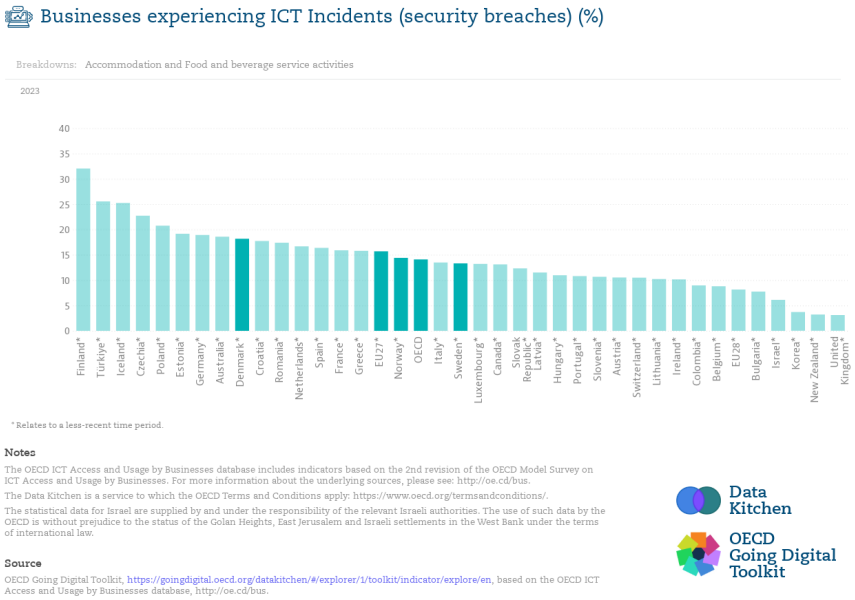
Ifølge DSB, har mat- og prosesseringsindustrien hatt hendelser der hele eller deler av ekom-systemet generelt og ERP-systemet spesielt, har vært ute av drift i perioder. [41]

Mat- og prosesseringsindustrien benytter i stor grad IT og OT-systemer for å støtte produksjon og distribusjon. En gjennomgang av risikofaktorer ved IT- og OT-systemer finnes i avsnittet om IT og OT i dypdykket om kraftbransjen.

Analysebyrået Radar spår at matindustrien blir mer sårbar nettopp fordi den operative teknologien som understøtter produksjonen har økt i omfang og kompleksitet, mens nødvendige cybersikkerhetstiltak for bedrifter i sektoren ikke i tilstrekkelig grad har blitt vurdert. Flere virksomheter må nå investere mer i sin risikostyring og dermed øke sin motstandskraft. Et eksempel på at motstandskraften i bransjen er utfordret ble synlig da Nortura i desember 2022 ble utsatt for et omfattende dataangrep. Dataangrepet medførte stengte IT-systemer og redusert aktivitet ved fabrikker.

IT-SIKKERHETSHENDELSER I EUROPA I MATVAREINDUSTRIEN

OECD har i sin verktøykasse «Going Digital» en oversikt over utviklingen innen digitalisering i Europa. Der kan oversikten brytes ned på sektornivå, og bransjer kan sammenlignes. [42]



Figuren viser prosentandelen av virksomheter innen mat- og overnatting som har opplevd cyberhendelser. 14,39 % av de spurte innen mat- og overnattingsbransjen har svart at de har vært utsatt for hendelser. Til sammenligning har 33.35 % av finans- og forsikring opplevd hendelser, en bransje som tradisjonelt har vært mer eksponert for hendelser, og dermed også sterkere regulert

[41] DSB, 2017: Risiko- og sårbarhetsanalyse av norsk matforsyning: https://www.dsbinfo.no/DSBno/2017/rapport/risiko-og-saarbarhetsanalyse-av-norsk-matforsyning/?page=42

[42] OECD Going Digital tooklit: https://goingdigital.oecd.org/datakitchen/#/explorer/1/toolkit/indicator/explore/en?mainCubeId=ICT_BUS&pairCubeId=ICT_BUS&sizeCubeId=&mainIndId=E3&pairIndId=E7&sizeIndId=&mainBreakdowns=CL_ICT_BUS_BRKD%3AACC&pairBreakdowns=CL_ICT_BUS_BRKD%3ABUS_TOTAL&sizeBreakdowns=&lollipop=&lollipopOpts=MAN.TRA.FIN&countries=DNK.E27.NOR.OECD.SWE&countryFilter=false&time=1230764400360.1640991600360&chart=barchart&fontSize=14&palette=normal&lastDates=true&timeScale=P1Y&flip=false&fullLabel=true

enn matindustrien. Norske selskaper innen mat- og overnatting har noe større andel cyberhendelser enn OECD-snittet, og noe lavere enn EU-snittet.

Nortura ble som nevnt rammet av et dataangrep. Selve hackingen ble oppdaget av Norturas egen sikkerhetsovervåkning. Det ble umiddelbart etablert nødløsninger for å opprettholde matkonsernets viktigste forretningsfunksjoner ved de over 30 produksjonsstedene. Den digitale delen av produksjonen ble erstattet med manuelle rutiner inn mot nyåret.[43] Kostnadene for håndteringen av angrepet ble rundt 36 millioner kroner. Dette viser konsekvensene ved dataangrep, og kostnaden kunne vært vesentlig verre om ikke beredskapsorganisasjonen i Nortura hadde agert så raskt.

DE 10 VANLIGSTE SÅRBARHETENE I NORSKE IT-SYSTEMER

Det finnes liten tilgjengelig oversikt over IT-sikkerheten i mat- og prosesseringsindustrien i Norge, men Nasjonal sikkerhetsmyndighet (NSM) har utarbeidet en oversikt over de **ti vanligste sårbarhetene** i norske IT-systemer, som vi benytter som en generell beskrivelse over sårbarheter i mangel av en særskilt beskrivelse av nåsituasjonen for mat- og prosesseringsindustrien spesifikt. Selv om listen inneholder sårbarheter i andre virksomheter enn mat- og prosesseringsindustri, vil antakelig flere av sårbarhetene også gjelde for matsektoren.

Listen inneholder sårbarhetene NSM oftest finner under inntrengingstester av graderte og ugraderte informasjonssystemer. NSMs rapport videreformidler disse sårbarhetene slik at norske virksomheter kan lære om dem og håndtere dem. For hver av sårbarhetene presenterer NSM også sikringstiltak med utgangspunkt i rådene i NSMs grunnprinsipper for IKT-sikkerhet. Inntrengningstestene, som ble foretatt i perioden 2020 til 2022, og avslører ti vanlige sårbarheter. Virksomhetene sårbarhetene er hentet fra, er underlagt *sikkerhetsloven* og hører blant annet hjemme i *forsvarssektoren, justissektoren og sentralforvaltningen*. Dette er en ikke-sortert liste.

Illustrasjon: Radar Norway. Kilde: Ti sårbarheter i norske IKT-systemer, NSM, 2023. [44]

NSM beskriver at de fleste sårbarhetene og årsakene har mye til felles. De fleste skyldes:

- mangelfull oversikt over egne systemer
- rutiner knyttet til passord- og brukerkontobehandling
- manglende oppdateringer av programvare og feilkonfigurasjon av tjenester

Vi kommer med noen anbefalinger til hvordan beslutningstakerne i matsektoren kan styrke sin motstandskraft og redusere sårbarhetene nevnt over i siste del av bransjeperspektivet.

---

[43] Dagligvarehandelen.no, lastet ned 14.04.24, kl 12:53: Dataangrepet på Nortura: – Intet digitalt system er uangripelig (dagligvarehandelen.no)

[44] Ti sårbarheter i norske IT-systemer: https://nsm.no/getfile.php/1313387-1700026023/NSM/Filer/Dokumenter/Rapporter/Ti%20s%C3%A5rbarheter%20i%20norske%20IKT-systemer.pdf

Utviklingen med økt antall cyberhendelser og tilhørende kostnader i EU, førte til at EU innførte nye regler for økt cybersikkerhet, og vi tar nå for oss de økte kravene til sikkerhet og rapportering som berører aktørene i mat- og prosesseringsindustrien. NIS2-direktivet og CER-direktivet gjør det enda viktigere for mat- og prosesseringsundustrien å styrke sin motstandskraft. De nye kravene vil medføre nye investeringer i kompetanse, systemer for risikohåndtering og ledelsesansvar.

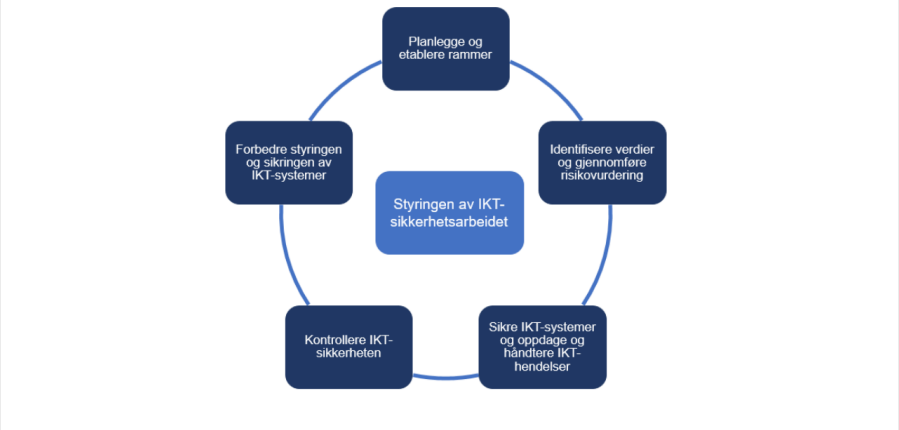
ANBEFALINGER TIL BESLUTNINGSTAKERE I MATSEKTOREN

Gjennomgangen ovenfor av nåsituasjonen for IT-sikkerhet i mat- og prosesseringsindustrien, samt relevant regelverk på området, viser noen områder der beslutningstakere bør rette oppmerksomheten for å **styrke motstandskraften og konkurransekraften** fremover. Dette er våre anbefalinger til hva beslutningstakere innen mat- og prosesseringsindustrien bør prioritere av tiltak fremover, der analyse av nåsituasjonen i virksomheten er essensielt for at tiltakene skal være tilpasset virksomhetens behov. Vi gir også generelle anbefalinger til beslutningstakere uavhengig av sektor helt til slutt i rapporten. Dette fordi den generelle økningen av reguleringer vil gi ringvirkninger på tvers av sektorer.

Vi anbefaler følgende:

1. **Innpass sikkerhet i virksomhetens aktiviteter og etablér styringssystem for informasjonssikkerhet**

   Virksomhetene bør integrere sikkerhet i virksomhetens aktiviteter og å etablere et styringssystem for informasjonssikkerhet som ivaretar systematikken for aktivitetene i IKT-sikkerhetsarbeidet. Dette kan illustreres slik:

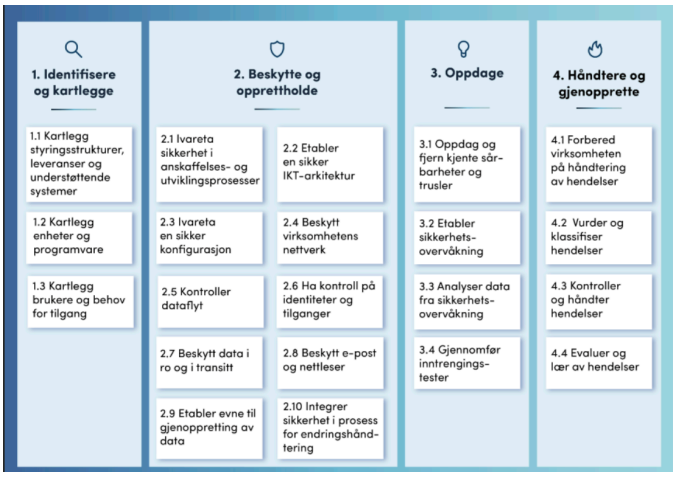


Illustrasjon av styringen av IKT-sikkerhetsarbeidet. Kilde: Riksrevisjonen, NSM og NVE.

Veiledninger til god sikkerhetsstyring kan finnes på Nasjonal sikkerhetsmyndighets sider. Det svenske mattilsynet har laget en veiledning for drikkevannsprodusenter, som også kan benyttes som god inspirasjon. [45]

[45] Livsmedelverket, 2023: Riskanalys som verktyg: https://www.livsmedelsverket.se/globalassets/publikationsdatabas/handbocker-verktyg/utbildningsmaterial-om-riskanalys-a_webb.pdf

2. Bruk NSMs grunnprinsipper for IKT-sikkerhet



NSMs grunnprinsipper for IKT-sikkerhet

Grunnprinsippene for IKT-sikkerhet gir råd for å beskytte informasjonssystemer, data og tjenester mot uautorisert tilgang, skade eller misbruk. Tilgjengelige støtteverktøy er blant annet digital veiledning, samt tilhørende Excel-fil for gjennomføring og prioritering av tiltak. [46]

3. Les NSMs rapport og tiltak mot de ti vanligste sårbarhetene i norske IT-virksomheter

NSM har identifisert de ti vanligste sårbarhetene i norske IT-virksomheter gjennom å utføre inntrengingstester i årene 2020-2022. [47] For hver av sårbarhetene presenterer NSM sikringstiltak med utgangspunkt i rådene i NSMs grunnprinsipper for IKT-sikkerhet.

4. Les NVEs veileder for risikovurderinger og informasjonssikkerhet i IT- og OT-systemer

Kilde: NVEs veileder for risikovurdering av IT og OT

Selv om fokuset er på IT og OT og for små og mellomstore virksomheter, egner risikovurderingsmetoden i veiledningen også for andre typer risikovurderinger og selskaper av alle størrelser. Veiledningen gir en trinnmodell for gjennomføring av risikovurderinger, og gir eksempler på hvordan kraftselskaper kan arbeide med å øke sin motstandskraft.[48]

5. Sørg for god IKT-sikkerhet i anskaffelser og tjenesteutsetting

Nasjonal sikkerhetsmyndighet har utarbeidet god veiledning knyttet til sikkerhetsfaglige anbefalinger ved tjenesteutsetting.[49]

---

[46] NSMs støtteverktøy for grunnprinsippene for IKT-sikkerhet: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/stotteprodukter/#:~:text=St%C3%B8tteverkt%C3%B8y%20for%20NSMs%20grunnprinsipper%20for%20IKT%2Dsikkerhet%202.0%C2%A0%20(XLSX%2C%20128KB)

[47] Ti sårbarheter i norske IT-systemer: https://nsm.no/getfile.php/1313387-1700026023/NSM/Filer/Dokumenter/Rapporter/Ti%20s%C3%A5rbarheter%20i%20norske%20IKT-systemer.pdf

[48] NVE veiledning, 2024: Veiledning for risikovurdering av IT og OT, skrevet av KPMG: https://publikasjoner.nve.no/veileder/2024/veileder2024_02.pdf

[49] NSM, sikkerhetsfaglige anbefalinger ved tjenesteutsetting: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/introduksjon/

6. **Gjennomgå minimumskravene i CER-direktivet og minimumstiltakene for cybersikkerhet ihht NIS2**

Virksomheter i matsektoren bør gjennomgå virksomhetens risikovurderinger, og utarbeide planer for motstandskraft. Det skal avholdes opplæring, og hendelser skal rapporteres. Tiltakene som skal gjennomføres av utpekte virksomheter etter CER-direktivet er:

Illustrasjon: Radar Norway, 2024. Kilde: Eurlex, Krav til kritiske enheters motstandsdyktighet (Kap III, artikkel 12-16).

Minimumstiltakene som må innføres i henhold til NIS2, også for norske virksomheter innen matindustrien dersom de overgår minimumskravene for størrelse og omsetning, er omtalt tidligere i rapporten, og omfatter følgende:

Virksomheter i matsektoren bør integrere dette arbeidet med minimumsaktivteter med tiltakene i punkt 1, **Innpass sikkerhet i virksomhetens aktiviteter og etablér styringssystem for informasjonssikkerhet.**

7. **Hold deg informert om kommende lover.**

Gjennomgangen av regelverkene er sammenfattet i Bilag A. Benytt oversikten til å forberede egen ledergruppe på virksomhetsstyringsaktiviteter som må planlegges. Kommende regler på cybersikkerhet, kritiske enheters motstandsdyktighet, samt cybersikkerhetsforordning og CER-direktivet peker seg ut for norske beslutningstakere.

OPPSUMMERING:

ANBEFALINGER TIL BESLUTNINGSTAKERE I MAT- OG PROSESSERINGSINDUSTRIEN

Beslutningstakere i mat- og prosseseringsindustrien bør gjøre flere grep for å **styrke motstandskraften og økt modenhet i risikostyring** fremover. Oppsummert kan våre anbefalinger visualiseres slik:

Anbefalinger til beslutningstakere i mat- og prosesseringsindustrien. Kilde: Radar 2024.

Våre funn for både energi- og kraftsektoren og mat- og prosesseringsindustrien viser at begge sektorer må investere i styrket motstandskraft. Analysebyrået Radar antar at det kreves større investeringer for mat- og prosesseringsindustrien enn for kraftindustrien, som følge av at det blir innført minimumskrav.

FORVENTET UTVIKLING INNEN IKT-SIKKERHET- KONSEKVENSER FOR ALLE SEKTORER

Oppsummert viser vår gjennomgang av det grunnet tette koblinger og avhengigheter, og rask innføring av ny teknologi, sammen med komplekse og lange verdikjeder i flere sektorer, gir økt omfang av reguleringer, økte angrepsflater og til sist et mer krevende sikkerhetsarbeid. Illustrasjonen nedenfor oppsummerer den forventede utviklingen på IKT-sikkerhet innen alle sektorer fremover.

Utviklingstrekk innen IKT-sikkerhet. Kilde: Radar Norway, 2024

Det blir altså et mye mer krevende sikkerhetsarbeid, som også gir konsekvenser på andre områder.

Utviklingen vi har vist gir ringvirkninger til andre sektorer. Derfor gir vi i det følgende anbefalinger til beslutningstakere som gjelder på tvers av sektorer.

FELLES ANBEFALINGER ALLE BESLUTNINGSTAKERE I NORSKE VIRKSOMHETER

Gjennomgangen av de generelle europeiske og de spesifikke norske reglene, forventet utvikling på IKT-sikkerhet og nåsituasjonen i både kraft- og energisektoren og mat- og prosesseringsiundustrien, viser at det er noen tiltak som alle sektorer nå bør gjøre. Her er våre generelle anbefalinger til norske beslutningstakere uavhengig av sektor.

VIRKSOMHETERS MOTSTANDSKRAFT MÅ ØKES (RESILIENCE)

Gjennomgangen av trusselbildet, nåsituasjonen og den regulatoriske utviklingen ovenfor, viser at det er et behov for å **styrke norske virksomheters motstandskraft i alle sektorer**. Definisjonen[50] vi benytter på motstandskraft er:

> "Motstandskraft er en organisasjons evne til å tilpasse seg endrede forhold, motstå forstyrrelser og komme seg raskt etter uheldige hendelser. I sammenheng med cybersikkerhet handler cybermotstandskraft spesielt om en organisasjons evne til å minimere virkningen av cyberhendelser og gjenopprette operative systemer for å opprettholde forretningskontinuitet.»

Kilde: Cisco, What is Cyber Resilience

ØKT PROFESJONALISERING AV RISIKOSTYRING I VIRKSOMHETER

De omtalte reglene gjør at arbeidet med minimumsnivåer for cybersikkerhet vil intensiveres i flere sektorer, og flere ansatte og ledere vil opparbeide seg kompetanse på risikostyring og prioritering av tiltak. Økt kompetanse vil også gi økt bestillerkompetanse på tjenester og rapportering internt, og med økt profesjonalisering kommer også økte krav til leveranser i ledergrupper. Flere IT-sikkerhetsansvarlige vil måtte styrke sin kompetanse, og flere ledere må tilegne seg styrket kompetanse på risikostyring slik at de kan kravstille leveranser bedre.

RISIKOSTYRING ER ET LEDELSESANSVAR!

De nye NIS2-reglene innebærer en tydeliggjøring av ledelsens ansvar, se spesielt artikkel 20 og 21 i NIS2-direktivet. Dette innebærer også at opplæringstiltak må innføres for ledelsen og styret, og at de kan stilles personlig ansvarlig for alvorlige brudd på reglene. Dette kan gjøre det enklere å prioritere sikkerhetsfaglige råd i virksomhetene, og kan bidra til at det blir enklere å sikre investeringer til nødvendige sikkerhetstiltak.

ØKT KAMP OM SIKKERHETSRESSURSER OG KOMPETANSE

Det forventes økt kamp om ressursene innen sikkerhetskompetanse, økt etterspørsel etter sikkerhetstjenester fra offentlig sektor som også forventes å omfattes av de nye NIS2-reglene, økt

[50] Cisco, What is cyber resilience: https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-cyber-resilience.html

etterspørsel etter sikkerhetstjenester i privat sektor som følge av flere omfattede bransjer, og økt etterspørsel etter nearshoring og offshoring som følge av at NIS2-regelverket gjelder for hele EU.

ØKTE KOSTNADER OG BEHOV FOR FLERE INVESTERINGER

Den økte tilsynsaktiviteten forventes å gi økte kostnader for virksomhetene, både i form av faktisk tilsynsaktivitet som skal tilrettelegges, avvik som må lukkes og mulige bøter i form av sanksjoner fra tilsynsmyndigheter. EUs egne tall antyder en kostnadsøkning på 22 % for de virksomheter som ikke tidligere har vært omfattet av NIS1, og en kostnadsvekst på 12 % for de virksomheter som fra før av er omfattet av NIS1. Direktivet innebærer også økte investeringer i opplæring og kompetanse, ikke bare på ledelsesnivå- men for alle ansatte.

ØKT BEHOV FOR KJØP AV «SECURE BY DESIGN» TJENESTER

Som følge av de store behov som kommer for å styrke motstandskraft i virksomheter i alle sektorer, vil det vokse frem et sterkere behov for kjøp av ferdig pakketerte «Secure by design»- tjenester. Dette er produkter der sikkerheten til kundene er et kjernekrav, ikke bare en teknisk funksjon. Prinsippene for Secure by Design bør implementeres under designfasen av et produkts utviklingslivssyklus for å dramatisk redusere antall utnyttbare feil før de introduseres til markedet for bred bruk eller forbruk.[51]

[51] America`s cyberdefence Agency, https://www.cisa.gov/securebydesign

BILAG A- REGULATORISK RAMMEVERK

2016-2019	2020-2021	2022-2024
Integritet & beskyttelse av data	**Digital suverenitet**	**Regulatoriske rammeverk**
GDPR US Cloud Act Schrems II	EU Strategy for Data	EU-US Data Privacy Framework EU Data Act EU AI Act EU Cybersecurity Act ENSIA Cloud Security Certification NIST Cybersecurity Framework CER-direktivet DORA-forordningen

Integritet & beskyttelse av data (2016–2019)	**GDPR**	Den generelle personvernforordningen (GDPR) trådte i kraft i 2018 og markerte starten på den strengeste personvern- og sikkerhetslovgivningen i verden. Denne forordningen setter en helt ny standard for personvernbestemmelser og lover.
	US Cloud Act	Europeiske selskaper som bruker en amerikansk skytjenesteleverandør for å lagre eller behandle dataene sine, kan være juridisk forpliktet til å dele disse dataene med amerikanske myndigheter i tilfelle etterforskning av alvorlige lovbrudd. Se også EU-U.S. Data Privacy Framework.
	Schrems II	Regulerer sikker overføring av personopplysninger fra EU til USA
Digital suverenitet (2020–2021)	**EU Strategy for Data**	EU:s digitale strategi omfatter flera lover: Data Governance Act for å håndtere data på att en tillitsvekkende måte og gjøre det enklere å dele data. Digital Markets Act leggedr til rette for mer rettferdige markeder for innovasjon, vekst og konkurransekraft i den digitale sektoren.
Regulatoriske ramverk (2022–2024)	**EU-US Data Privacy Framework**	Data Privacy Framework 2023 skal sikre at sensitive og kritiske data beskyttes for å forbedre digital suverenitet for virksomheter i Europa og over hele verden.
	EU Data Act	EU:s Data Act skal sikre rettferdighet gjennom å overholde regler for bruk av data som genereres av Internet of Things (IoT) – enheter.
	EU AI Act	Spredning av av data og det økende antall nye AI-system har gitt opphav til denne reguleringen. Målet med AI-loven er å regulere AI-tilpasninger og tilpasse den til EUs overgripende verdier og grunnleggede rettigheter.
	EU Cybersecurity Act	Med de seneste årenes økende cybersikkerhetstrusler har EU lansert flere forordninger og initiativ for å beskytte borgerne og virksomhetenes sikkerhet og integritet. EU Cybersercurity Act øker det operative samarbeidet på EU-nivå ved store grenseoverskridende cyberangrep ogkriser.
	ENISA Cloud Security Certification	ENISA bidrar til EU:s cyberreguleringer, styrker tilliten til IKT - produkter, tjenester og prosesser med cybersikkerhetssertifisering.
	NIST Cybersecurity Framework	NIST hjelper virksomheter av alle størrelser med å forstå, håndtere og redusere sin cybersikkerhetsrisiko, og beskytte

	nettverk og data. Rammeverket er frivillig for virksomhetene å følge.
CER-direktivet	CER-direktivet stiller krav til tiltak for å styrke motstandskraften i viss samfunnskritisk virksomhet.
DORA-forordningen	DORA-forordningen skal bidra med en økt digital operativ motstandskraft i EU:s finanssektor. Det omhandler implementering av regler, verktøy og rammeverk for risikohåndtering, rapportering og testing for å minimere risikoen og eventuelle konsekvenser ved IKT-relaterte hendelser.
NIS2-direktivet	NIS 2 direktivet skal heve minimumsnivået på sikkerhetsområdet i alle EUs medlemsland – både fysisk og digitalt. Direktivet betyr at norske organisasjoner-både private og offentlige- er ansvarlige for å sikre at sikkerheten i hele forsyningskjeden er NIS2-kompatibel. NIS2 krever systematisk due diligence, rapportering og ledelsesfokus
Cyber Resilience Act	Forordning om horisontale cybersikkerhetskrav for produkter med digitale elementer. Produkter som dekkes av forordningen er bredt og vil gjelde alt fra eksempelvis smartklokker og leketøy til rutere og brannmurer samt programvare som benyttes i produktene. Lovforslaget skal redusere sårbarheter i produkter som plasseres på markedet i EU/EØS, og sikre at produsenter blir ansvarlige for cybersikkerheten i produktene gjennom hele produktets livssyklus. Reguleringen er ment å komplementere kravene i det grunnleggende EU cybersikkerhetsrammeverket i EU, Directive on the Security of Network and Information Systems (NIS2) og EU Cybersecurity Act.

Faglige bidragsytere fra Cisco i arbeidet med denne rapport:

Bjorn A. Wentzel
Linn C. Bye
Monica Sylvander
Merete Asak
Trine Strømsnes
Mari Orbak
Henrik Parnemann
Mads Lindback
Nikolai Kaldahl-Miller
Frank Tuhus
Arne Martin Skyrud
Ann Katrine Kolstad
Kent Antonsen
Charlotte Hovring
Geir Arne Nordtveit